

UNCLASSIFIED



ZEBRA TECHNOLOGIES ANDROID 14 STIG SUPPLEMENTAL PROCEDURES

30 September 2026

Developed by Zebra Technologies and DISA for the DoW

UNCLASSIFIED

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
1. ZEBRA TECHNOLOGIES ANDROID 14 DEVICE	1
1.1 Zebra Device Overview	1
1.2 Zebra Android Enterprise Compliance	3
2. ZEBRA ANDROID SECURITY OVERVIEW.....	5
2.1 Zebra Android Operating System.....	5
2.1.1. Security-Enhanced Linux (SELinux).....	5
2.1.2. Trusted Execution Environment.....	5
2.2 LifeGuard for Android – Over-the-Air Updates.....	5
3. ANDROID ENTERPRISE.....	6
3.1 EMM/MDM Console	6
3.2 DPC (Device Policy Controller).....	6
3.3 Work Profile Security.....	6
3.3.1. COPE Deployments and User Privacy.....	7
3.3.2. Managed Configuration.....	7
4. DEVICE CONFIGURATION.....	8
5. PROCEDURES	9
5.1 Device Wipe.....	9
6. SPECIAL GUIDANCE	10
6.1 Zebra Android Device Disposal	10
6.2 Configuration of the Personal Space.....	10
7. DOW PKI PUREBRED	11
8. ADDITIONAL CONSIDERATIONS.....	12
8.1 Wearables.....	12
8.2 Google Location Tracking.....	12

LIST OF TABLES

	Page
Table 1-1: Zebra Devices.....	1

LIST OF FIGURES

	Page
Figure 3-1: Components of an Android Enterprise Solution	6
Figure 4-1: Personal Profile and Work Profile	8

1. ZEBRA TECHNOLOGIES ANDROID 14 DEVICE

1.1 Zebra Device Overview

Zebra offers 68 different models of its Zebra Android 14 device. The models, from handhelds and tablets to wearables and vehicle-mounted computers, equip DoW workers for a variety of use cases. Zebra's Android 14 devices feature robust built-in software intelligence with integrated scanning capabilities.

Table 1-1: Zebra Devices

Model #	CPU	Wireless Chipset	Cellular	Wi-Fi 6 Support	Description
SDM660 Devices with WCN3990					
CC600	SDM660	WCN3990	WLAN	No	5" Customer concierge interactive tablet-style kiosk device
CC6000	SDM660	WCN3990	WLAN	No	10" Customer concierge interactive tablet-style kiosk device
ET51	SDM660	WCN3990	WLAN	No	8"/10" Tablet
ET56	SDM660	WCN3990	WWAN Data Only	No	8"/10" Tablet
L10A	SDM660	WCN3990	WWAN Data Only	No	10" Ultra-rugged WWAN tablet
MC20	SDM660	WCN3990	WLAN	No	4" Keypad WLAN device for Japanese market
MC9300	SDM660	WCN3990	WLAN	No	4.3" Ultra-rugged keypad WLAN device
PS20	SDM660	WCN3990	WLAN	No	4" Personal Shopper assistant
TC52	SDM660	WCN3990	WLAN	No	5" Phone
TC52-HC	SDM660	WCN3990	WLAN	No	5" Phone made from healthcare grade plastics
TC52x	SDM660	WCN3990	WLAN	No	5" Phone
TC52x-HC	SDM660	WCN3990	WLAN	No	5" Phone made from healthcare grade plastics
TC57	SDM660	WCN3990	WWAN/ Cellular	No	5" Phone
TC57x	SDM660	WCN3990	WWAN/ Cellular	No	5" Phone
TC72	SDM660	WCN3990	WLAN	No	4.7" Ultra-rugged phone
TC77	SDM660	WCN3990	WWAN/ Cellular	No	4.7" Ultra-rugged phone
TC83	SDM660	WCN3990	WLAN	No	4" Ultra-rugged touch computer/gun handler phone
VC83	SDM660	WCN3990	WLAN	No	8"/10" Vehicle-mounted computer
WT6300	SDM660	WCN3990	WLAN	No	3.2" Advanced glove-optimized rugged wearable device
EC30	SDM660	WCN3990	WLAN	No	3" Portable, lightweight phone
EC50	SDM660	WCN3990	WLAN	No	5" Enterprise Mobile computer with optional integrated scanner
EC55	SDM660	WCN3990	WWAN/ Cellular	No	5" Enterprise Mobile computer with optional integrated scanner
MC2200	SDM660	WCN3990	WLAN	No	4" Touch computer/gun handler
MC2700	SDM660	WCN3990	WWAN/ Cellular	No	4" Touch computer/gun handler
MC3300x	SDM660	WCN3990	WLAN	No	4" Touch computer/gun handler
MC33xR	SDM660	WCN3990	WLAN	No	4" Touch computer/gun handler with RFID
SDM660 Devices with WCN3980					
TC21	SDM660	WCN3980	WLAN	No	5" Phone

Model #	CPU	Wireless Chipset	Cellular	Wi-Fi 6 Support	Description
TC21-HC	SDM660	WCN3980	WLAN	No	5" Phone made from healthcare-grade plastics
TC26	SDM660	WCN3980	WWAN/ Cellular	No	5" Phone
TC26-HC	SDM660	WCN3980	WWAN/ Cellular	No	5" Phone made from healthcare-grade plastics
SDM660 Devices with BCM43752					
TC52ax	SDM660	BCM43752	WLAN	Yes	5" Phone
MC33ax	SDM660	BCM43752	WLAN	Yes	4" Touch computer/gun handler
QCM4490/QCS4490 Devices with WCN6856					
MC3400	QCM4490	WCN6856	WLAN	Yes	4.0" Gun, straight shooter scanning device
MC3450	QCM4490	WCN6856	WWAN	Yes	4.0" Gun, straight shooter scanning device
MC9400	QCM4490	WCN6856	WLAN	Yes	4.3" Ultra-rugged pistol grip device
MC9450	QCM4490	WCN6856	WWAN	Yes	4.3" Ultra-rugged pistol grip device
PS30	QCM4490	WCN6856	WLAN	Yes	4.7" Shopping device
TC53e	QCM4490	WCN6856	WLAN	Yes	6" Phone
TC58e	QCM4490	WCN6856	WWAN	Yes	6" Phone
FR55 / FR55S	QCS4490	WCN6856/ SDR435 (WWAN)	WWAN	Yes	True hot swap, NFC, secure element, SAM phone
WT5400	QCS4490	WCN6856	WLAN	Yes	4.7" Wearable
WT6400	QCS4490	WCN6856	WLAN	Yes	4.7" Wearable
QCM5430 Devices with WCN6856					
HC20	QCM5430	WCN6856	WLAN	Yes	6" Phone made from healthcare-grade plastics
HC50	QCM5430	WCN6856	WLAN	Yes	6" Phone made from healthcare-grade plastics
TC22	QCM5430	WCN6856	WLAN	Yes	6" Phone
TC27	QCM5430	WCN6856	WWAN/ Cellular	Yes	6" Phone
TC22R	QCM5430	WCN6856 (WIFI)	WLAN only	Yes	6" Gun-style phone with NFC
TC27R	QCM5430	WCN6856 (WIFI) SDR735 (WWAN, GPS)	WWAN	Yes	6" Gun-style phone with NFC
EM45	QCM5430	WCN6856 (WIFI) SDR735 (WWAN, GPS)	WWAN	Yes	6.7" Phone with 5G Sub6, NFC, BLE 5.3
TC73-5430	QCM5430	WCN6856	WLAN	Yes	Phone (Nazare)
TC78-5430	QCM5430	WCN6856 (WIFI) SDR735 (WWAN, GPS)	WWAN	Yes	Phone (Nazare)
KC50S	QCM5430	WCN6856	WLAN	Yes	22" & 15" Tablet with NFC
KC50L	QCM5430	WCN6856	WLAN	Yes	22" & 15" Tablet with NFC
HC25	QCM5430	WCN6856 (WIFI) SDR735 (WWAN, GPS)	WWAN	Yes	22" & 15" Tablet with NFC

Model #	CPU	Wireless Chipset	Cellular	Wi-Fi 6 Support	Description
HC55	QCM5430	WCN6856 (WIFI) SDR735 (WWAN, GPS)	WWAN	Yes	22" & 15" Tablet with NFC
ZEC500	QCM5430	WCN6856	WLAN	Yes	Wireless WSC, Kisok box – Android device without an embedded display or battery
SM6375 Devices with BCM43752					
ET40	SM6375	BCM43752	WLAN	Yes	8"/10" Tablet with NFC PN7160
ET40HC	SM6375	BCM43752	WLAN	Yes	8"/10" Tablet made from healthcare-grade plastics, NFC PN7160
ET45	SM6375	BCM43752	WWAN Data Only	Yes	8"/10" Tablet with NFC PN7160
ET45HC	SM6375	BCM43752	WWAN Data Only	Yes	8"/10" Tablet made from healthcare-grade plastics, NFC PN7160
SM6375 with WCN3988					
TC15	SM6375	WCN3988	WWAN/ Cellular	No	6.5" Phone with NFC PN557
TN28	SM6375	WCN3988	WWAN/ Cellular	No	6.5" Phone with NFC PN557
QCM6490 Devices with WCN6856					
ET60	QCM6490	WCN6856	WLAN	Yes	10" Tablet
ET65	QCM6490	WCN6856	WWAN Data Only	Yes	10" Tablet
TC53	QCM6490	WCN6856	WLAN	Yes	6" Phone
TC58	QCM6490	WCN6856	WWAN/ Cellular	Yes	6" Phone
TC73	QCM6490	WCN6856	WLAN	Yes	6" Phone
TC78	QCM6490	WCN6856	WWAN/ Cellular	Yes	6" Phone

The above models may represent additional model-specific SKUs that vary by screen size, RAM/storage capacity, battery capacity, or base versus premium materials. The Bluetooth Message Access Profile (MAP) is not supported on devices without cellular capabilities. Some of the claimed SKUs (e.g., TC58e, TC53e) are equipped with Strongbox capabilities.

1.2 Zebra Android Enterprise Compliance

Zebra devices are fully compliant with Google Mobile Services (GMS) and are certified for GMS before publishing each official release. Zebra devices that use Android 14 are also certified as Android Enterprise Recommended (AER) rugged devices. This implies that any Mobile Device Management (MDM) system certified for enterprise can be used on the Zebra devices. The customer can choose any of the MDMs and use those to configure the Zebra devices.

Zebra devices are fully compliant with Android Enterprise enrollment methods, including QR Code, NFC, Google Account, and Zero-Touch. Zero-Touch enrollment is a deployment method that allows administrators to configure devices at scale with minimal user intervention. This method ensures improved management and control by automating the enrollment process. It is particularly useful for deploying large numbers of devices across an organization while maintaining consistency

in security configurations. Administrators can preconfigure device settings, apps, and policies before distribution to end users, streamlining operational efficiency and compliance.

2. ZEBRA ANDROID SECURITY OVERVIEW

2.1 Zebra Android Operating System

Zebra customizes the Android open-source operating system (OS) 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 OS through a framework that describes system services, platform application programming interfaces (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 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 implemented using ARM TrustZone technology.

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

- Lock screen passcode verification.
- Biometric template matching.
- Protection and management of Keystore keys.

2.2 LifeGuard for Android – Over-the-Air Updates

[LifeGuard for Android Over-the-Air \(OTA\)](#) 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 the software.

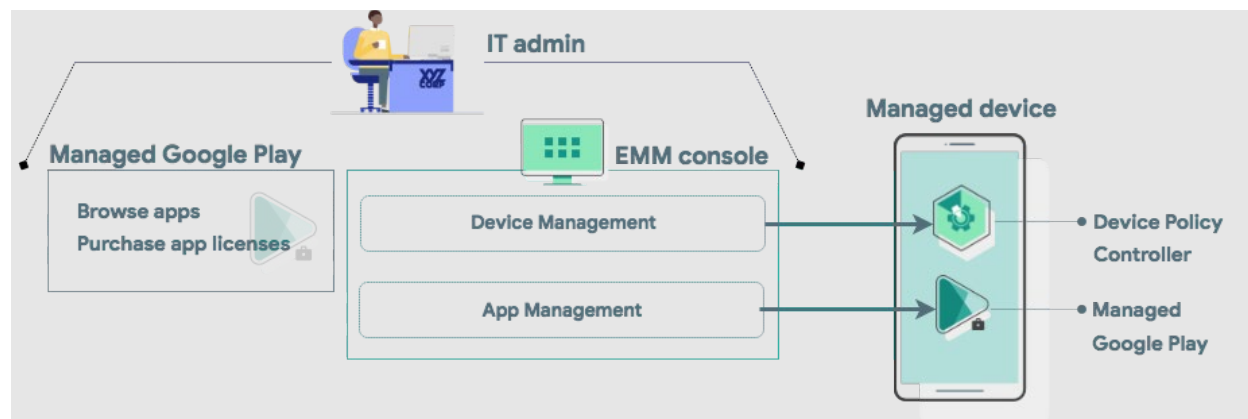
Administrators of fully managed devices can install system updates via a system update file. Manual system updates allow IT administrators to:

- Test an update on select devices before installing them widely.
- Avoid duplicate downloads on bandwidth-limited networks.
- Stagger installations or update devices only when not in use.

3. ANDROID ENTERPRISE

An Android Enterprise solution is a combination of three components: the Enterprise Mobility 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 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 device policy controller (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 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 show up 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 remove it only by removing the entire work profile. Administrators can remotely instruct the device policy client to remove the work profile, for instance, when 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

Zebra 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 must be used to permit or block specific applications from use in the personal profile. It is highly recommended that DoW 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.

3.3.2. Managed Configuration

Managed configurations, using a standard mechanism, allow the organization's IT administrator to specify settings for apps remotely. Zebra OEMConfig is Zebra's Original Equipment Manufacturer (OEM)-specific application that conforms to the OEMConfig model. This model enhances the managed configuration mechanism to allow device configuration through the OEMConfig application. It provides access to Zebra-specific and privileged functions via Managed Configurations exposed by the Zebra OEMConfig application.

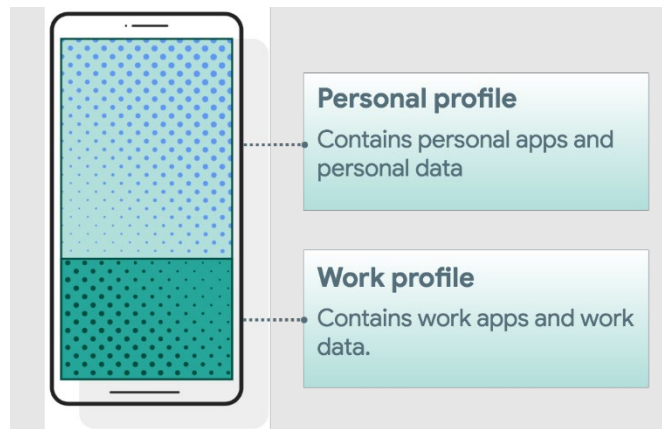
The OEMConfig schema provides the information necessary for an EMM to display an organized user interface to allow the IT administrator a simple way to configure devices. Zebra's OEMConfig exposes more than 600 managed configurations spanning display settings, application settings, system settings, and beyond. An EMM DPC enrolled as a device owner or profile owner can be used to set policies and/or managed configuration values on a device.

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

Zebra Android devices can be wiped by a factory data reset, through 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 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 Zebra Android Device Disposal

Follow the procedure below prior to disposing of (or transferring to another user) Zebra 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

DoW 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 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 (AE) 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 DoW 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 ZEBR-14-009800 for more information.

7. DOW 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 DoW PKI subscribers' use on commercial mobile devices.

Requirements for Zebra Android devices credentialed using DoW PKI Purebred are as follows:

- Users are responsible for maintaining positive control of their credentialed devices; the DoW 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 DoW-owned Zebra Android 14 device is prohibited. VR wearables are considered a personal use product with no DoW mission requirement.

8.2 Google Location Tracking

DoW policy memorandum “Use of Geolocation-Capable Devices, Applications, and Services,” 03 August 2018, prohibits the use of geolocation-capable devices, applications, and services on DoW mobile devices in designated operational areas (OAs). Independent researchers and DISA analysis have determined that even when Location History is disabled, Android continues to store location data on the mobile device¹. Therefore, AOs should consider additional actions to limit Google tracking mobile devices when these devices are operated in OAs.

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.