



# ZEBRA ANDROID 11 COBO SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

## Version 1, Release 3

## 25 October 2023

## Developed by Zebra Technologies and DISA for the DOD

## Trademark Information

# TABLE OF CONTENTS

**Page**

# LIST OF TABLES

**Page**

# LIST OF FIGURES

**Page**

# 1. INTRODUCTION

## 1.1 Executive Summary

The Zebra Android 11 Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to Zebra Technologies handheld devices running Android 11 that process, store, or transmit unclassified data marked as "Controlled Unclassified Information (CUI)" or below.

This STIG leverages the Google Android 11 STIG. All requirements in this STIG are based on the Google Android 11 STIG, with several changes specific to Zebra Technologies.

The scope of this STIG covers the Corporate Owned Business Only (COBO)[1] use case. The Corporate Owned Personally Enabled (COPE), Bring Your Own Device (BYOD), and Bring Your Own Approved Device (BYOAD)[2] use cases are not in scope for this STIG.

**Note**: If the Authorizing Official (AO) has approved the use/storage of DOD data in one or more personal (unmanaged) apps, allowing unrestricted user activity in downloading and installing personal (unmanaged) apps on Zebra Technologies devices may not be warranted due to the risk of possible loss of or unauthorized access to DOD data.

This STIG assumes that if a DOD Wi-Fi network allows Zebra Technologies devices to connect to the network, the Wi-Fi network complies with the Network Infrastructure STIG; for example, wireless access points and bridges must not be connected directly to the enclave network.

## 1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that "all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be […] configured […] consistent with applicable DOD cybersecurity policies, standards, and architectures." The instruction tasks that DISA "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

[1] Work data/apps only – no personal data/apps
[2] BYOAD is the DODs term for Choose Your Own Device (CYOD), which is similar to BYOD, but only select models of personal devices are allowed.

## 1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

**Table 1-1: Vulnerability Severity Category Code Definitions**

| | DISA Category Code Guidelines |
|---|---|
| CAT I | Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity. |
| CAT II | Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity. |
| CAT III | Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity. |

## 1.4 STIG Distribution

Parties within the DOD and federal government's computing environments can obtain the applicable STIG from the DOD Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from https://public.cyber.mil/.

## 1.5 MDFPP Compliance Reporting

All Mobile Device Fundamentals Protection Profile (MDFPP) and DOD Annex security functional requirements (SFRs) were considered while developing this STIG. In DOD environments, devices must implement SFRs as specified in the DOD Annex to the MDFPP.

Requirements that are applicable and configurable are included in this STIG.

## 1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

## 1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

### 1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (https://www.niap-ccevs.org/) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DOD mandated standards.
- DOD Unified Capabilities (UC) Approved Products List (APL) (https://www.disa.mil/network-services/ucco) IAW DODI 8100.04.

# 2. ZEBRA TECHNOLOGIES ANDROID 11 DEVICE

## 2.1 Zebra Device Overview

Zebra offers 37 different models of its Zebra Android 11 device. The models—from handhelds and tablets to wearables and vehicle-mounted computers, equip DOD workers for a variety of use cases. Zebra's Android 11 devices feature robust built-in software intelligence with integrated scanning capabilities.

- Handheld computer models: EC30, EC50, EC55, MC9300, MC2200, MC2700, PS20, MC3300x, MC33ax, MC20
- Touch computer models: TC21, TC26, TC52, TC52x, TC52ax, TC57, TC57x, TC72, TC77, TC8300
- Tablets: ET40, ET45, ET51, ET56, L10A
- Wearable: WT6300
- RFID scanner: MC33xR
- Healthcare Touch computers models: TC21-HC, TC26-HC, TC52-HC, TC52x-HC, TC52ax-HC
- Vehicle-mounted device: VC8300
- Interactive kiosks: CC600, CC6000

## 2.2 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 11 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.

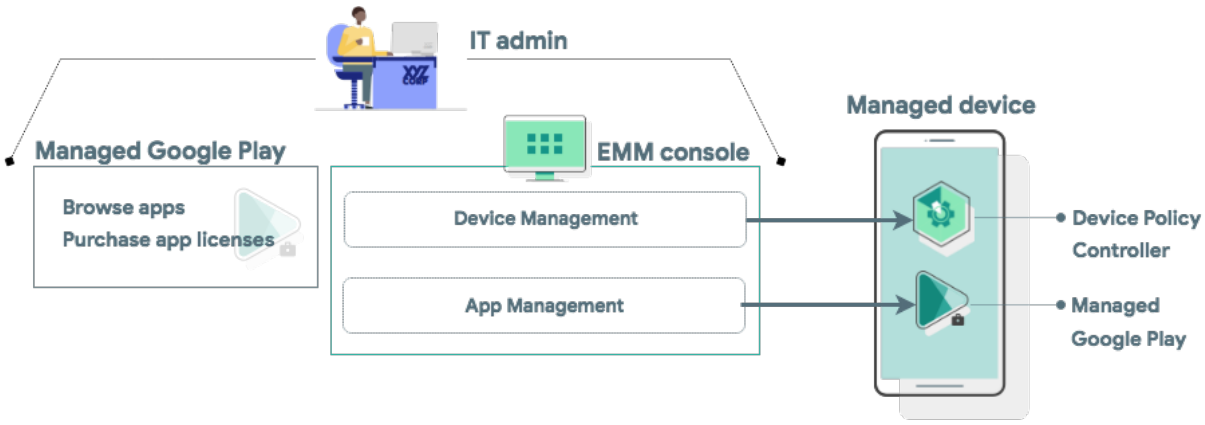
Zebra devices are fully compliant with Android Enterprise enrollment methods, including QR Code, NFC, Google Account, and Zero-Touch. Zero-Touch simplifies the out-of-the-box experience and enables enterprise customers to automatically provision devices they own with no administrator/user action required.

Details about the enterprise program and different components can be found in Android documentation.

## 2.3 Zebra Device Management

Zebra devices leverage the device management capabilities provided through Android Enterprise, which is a combination of three components: The Enterprise Mobility Management (EMM)/MDM console; a device policy controller (DPC), which is the MDM Agent; and an EMM/MDM Application Catalog.

**Figure 2-1: Components of an Android Enterprise Solution**




## 2.4 EMM Console

EMM solutions typically take the form of an EMM console—a web application the organization develops that allows IT administrators to manage their organization, devices, and apps. To support these functions for Android, integrate the console with the APIs and UI components provided by Android Enterprise.

## 2.5 DPC (EMM Agent)

All Android devices that an organization manages through the EMM console must install a DPC application 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 selected, the EMM solution can be coupled with the EMM solution's DPC, Android's DPC, or with a custom DPC that the organization develops.

End users can provision a fully managed or dedicated device using a DPC identifier (such as "afw#") 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.
- Once installed, the EMM's DPC must guide the user through the process of provisioning a fully managed or dedicated device.

## 2.6 Managed Configuration

Managed configurations allow the organization's IT administrator to specify settings for apps remotely. "Zebra OEMConfig" is Zebra's OEM-specific application that conforms to the OEMConfig model. It provides access to Zebra-specific and privileged functions via Managed Configurations that are exposed by the Zebra OEMConfig application.

Use EMM DPC enrolled as a device owner to set EMM policies or managed configuration values on a device.

## 2.7 Security Logging

IT administrators can gather, parse, and programmatically evaluate usage data from devices to identify malicious or risky behavior. Activities logged include Android Debug Bridge (ADB) activity, application launches, and screen unlocks. For Audit Logging, IT administrators can do the following:

- Enable security logging for target devices, and the EMM's DPC must be able to retrieve both security logs and pre-reboot security logs automatically.
- Review enterprise security logs for a given device and configurable time window in the EMM's console.
- Export enterprise security logs from the EMM's console.
- Capture relevant logging information from Logcat, which does not require any additional configuration to be enabled.
- Audit events from the Security Log are those where the "Keyword" field appears first in the format. For example: `<Keyword> (<Date><Timestamp>): <message>`

**IMPORTANT: EMM DPC enable security logging must be used to meet Common Criteria (CC) compliance.**

Zebra has additional managed configurations that must be audit logged according to DOD Annex for MDF PP 3.1.

Zebra performs additional security audit logging through OEMConfig, which leverages existing Google APIs already compatible to CC standards, to write it to security logs. Zebra security log entry produces the following information:

- Tag:
  Zebra is using custom TAG for audit logging:
  `TAG_MANAGE_CONFIGURATION_APPLIED = 1111111`
- Message:
  A string message includes date, time, caller name, title of the managed configuration, results (success or failure of applying the managed configuration, and failure reason if results lead to failure.

## 2.8 Logcat Logs

Logcat logs can be read by a command issued via an ADB shell running on the phone. Information about reading Logcat logs can be found at developer.android.com/studio/command-line/logcat. The command to issue a dump of the logcat logs is:

```
> adb logcat
```

Logcat logs cannot be exported from the device outside of using the ADB command shown above to dump to a file and then retrieving the file from the device (which requires developer settings to be enabled and administrative permissions).

Logcat logs can also be read by an application (for example an MDM agent) granted permission from an ADB shell:

```
> adb shell pm grant <application_package_name> android.permission.READ_LOGS
```

Audit events from the Logcat log are those where the "Keyword" field appears after the timestamp field in the format.

Example: `<Date> <Time> <ID> | <Keyword> <Message>`