

UNCLASSIFIED



**SAMSUNG ANDROID OS 11 WITH KNOX 3.X
SECURITY TECHNICAL IMPLEMENTATION GUIDE
(STIG) OVERVIEW**

Version 1, Release 1

20 November 2020

Developed by Samsung and DISA for the DoD

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 DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

	Page
1. INTRODUCTION.....	5
1.1 Executive Summary	5
1.2 Authority	6
1.3 Vulnerability Severity Category Code Definitions	6
1.4 STIG Distribution.....	7
1.5 MDFPP Compliance Reporting	7
1.6 Document Revisions	7
1.7 Other Considerations.....	7
1.8 Product Approval Disclaimer.....	8

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions	7

1. INTRODUCTION

1.1 Executive Summary

The Samsung Android OS 11 with Knox 3.x Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to Samsung Android 11 with Knox devices.

In October 2021, DISA plans to release updates to all current Samsung Android STIGs, which will ban the use of Android legacy deployments due to end of support by Google for legacy mobile device manager (MDM) management. In addition, the Samsung Android 12 STIG (expected to be released in late 2021) will include only Android Enterprise (AE) deployment. All Samsung phones that can support AE, which are currently deployed using legacy management APIs, should be upgraded to AE as soon as possible, and Samsung phones that cannot support AE should be replaced before October 2021.

The scope of this STIG covers only the Corporate Owned Personally Enabled (COPE) and Corporate Owned Business Only (COBO)¹ use cases. The Bring Your Own Device (BYOD) and Choose Your Own Device (CYOD)² use cases are not in scope for this STIG. In addition, the STIG supports two different Knox Platform for Enterprise (KPE) device deployment modes: Legacy and AE.

Note: It is expected that a future Samsung Android STIG will require all DoD deployments to use AE deployments only. It is recommended that DoD mobile service providers support AE deployments to the maximum extent possible now.

This STIG assumes that for the COPE use case, the technology used for data separation between work apps and data as well as personal apps and data has been certified by the National Information Assurance Partnership (NIAP) as compliant with the data separation requirements of the Protection Profile for Mobile Device Fundamentals (MDF)³.

The configuration requirements and controls implemented by this STIG allow unrestricted user activity in downloading and installing personal apps and data (music, photos, etc.) with Authorizing Official (AO) approval and within any restrictions imposed by the AO for the COPE use case. See the STIG Supplemental document (Section 8, Configuration of the Personal Environment), for more information. This STIG assumes that if a DoD Wi-Fi network allows a Samsung mobile device 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.

With AO approval, this STIG allows fingerprint biometric authentication for device unlock and work profile/workspace unlock. The fingerprint biometric method has successfully passed a Common Criteria evaluation using the Protection Profile for MDF v3.1 for the previous version

¹ Work data/apps only; no personal data/apps.

² Similar to BYOD; only a select number of personal devices are allowed.

³ The primary Protection Profile requirement is FDP_ACF_EXT.1.2.

of the Samsung platform (Android 10) and will be reviewed again during the Samsung Android 11 Common Criteria evaluation. Other Samsung-supported biometric methods are not approved, including facial recognition and trust agents.

Knox Mobile Enrollment (KME) enables large-scale Samsung Android device deployments so organizations can mobilize their employees with ease. KME allows DoD mobile service providers to deploy corporate-owned devices in bulk without having to manually set up each device. It is recommended that DoD mobile service providers consider deploying all Samsung devices via KME to improve enterprise management, control, and enrollment of DoD-owned Samsung devices. See the STIG Supplemental document (Section 5.2.2, Knox Mobile Enrollment) for more information. Samsung Android devices are also compatible with AE zero-touch service, which offers similar functionality to Samsung's KME.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that “all IT that receives, processes, stores, displays, or transmits DoD information will be [...] configured [...] consistent with applicable DoD cybersecurity policies, standards, and architectures” and tasks that Defense Information Systems Agency (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, 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 need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

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 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 Authorizing

Official. 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 Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured 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). DoD Authorizing Officials (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 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/projects/cryptographic-module-validation-program>) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (<http://www.disa.mil/network-services/ucco>) IAW DoDI 8100.04