MICROSOFT ANDROID 11
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 1

09 November 2022

Developed by Microsoft and DISA for the DOD

Trademark Information

TABLE OF CONTENTS

Page

1. INTRODUCTION 1

1.1 Executive Summary 1
1.2 Authority 1
1.3 Vulnerability Severity Category Code Definitions 2
1.4 STIG Distribution 2
1.5 MDFPP Compliance Reporting 2
1.6 Document Revisions 2
1.7 Other Considerations 3
1.8 Product Approval Disclaimer 3

2. ASSESSMENT CONSIDERATIONS 4

2.1 Surface Duo 2 Overview 4
2.2 Surface Duo 2 Description 4
2.3 Surface Duo 2 in the Enterprise 4
2.3.1 Surface Duo 2 Management Overview 4
2.4 Surface Duo 2 Security Overview 6
2.4.1 Mobile Device Management Security 7
2.4.2 Surface Duo 2 NIAP MDFPP and Commercial Solutions for Classified (CSfC) Compliance 7
2.4.3 Surface Duo 2 Auditing and Logging 8

LIST OF TABLES

Page

Table 1-1: Vulnerability Severity Category Code Definitions 2
Table 2-1: Managing Personally Owned Surface Duo 2 Devices 5
Table 2-2: Managing Corporate-Owned Surface Duo 2 Devices 5
Table 2-3: Microsoft Surface Duo 2 NIAP Compliance 8

LIST OF FIGURES

Page

Figure 2-1: Surface Duo 2 Device 4

1. INTRODUCTION

1.1 Executive Summary

The Microsoft Android 11 Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to Microsoft Android devices running Android 11 that process, store, or transmit unclassified data marked as "Controlled Unclassified Information (CUI)" or below. The STIG is based on the Protection Profile for Mobile Device Fundamentals (MDFPP) version 3.1 STIG Template.

The scope of this STIG covers both 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.

This STIG assumes that for the COPE use case, the technology used for data separation between work apps, data and personal apps, and data that has been certified by the National Information Assurance Partnership (NIAP) is compliant with the data separation requirements of the MDFPP[3]. As of the publication date of this STIG, the only data separation technology or application that is NIAP-certified for a Microsoft Android 11 device is the native Android Enterprise personal profile/work profile technology.

This STIG leverages the Google Android 11 STIG. All requirements in this STIG are based on the Google Android 11 STIG with several Microsoft-specific changes.

Note: This STIG requires that a NIAP-approved version of Android 11 be installed on DOD-owned Microsoft Android devices.

This STIG assumes that if a DOD Wi-Fi network allows a Microsoft 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.

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.

[1] Work data/apps only – no personal data/apps
[2] Similar to BYOD, but only select models of personal devices are allowed.
[3] The primary Protection Profile requirement is FDP_ACF_EXT.1.2.

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.

1.3 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

Category	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. ASSESSMENT CONSIDERATIONS

2.1 Surface Duo 2 Overview

The Microsoft Surface Duo 2 is a dual-screen Android 11 device that can be configured during initial deployment for either the COBO use cases (also called Device Owner) or the COPE use cases (Profile Owner).

2.2 Surface Duo 2 Description

The Android 11 operating system includes a Linux 5.4.86 kernel. Additional libraries are provided to developers to help ensure secure application development and use for features such as Sensitive Data Protection.

Figure 2-1: Surface Duo 2 Device

2.3 Surface Duo 2 in the Enterprise

Microsoft Surface Duo 2 is Google Mobile Services (GMS) compliant and can be managed via the Android Management API. This means any MDM leveraging this API can manage the Surface Duo 2.

Surface Duo 2 can be provisioned with a variety of enrollment mechanisms, including QR Code and NFC for both COBO and COPE provisioning. Additionally, Zero-Touch enrollment can be used to streamline the out-of-the-box experience.

2.3.1 Surface Duo 2 Management Overview

Commercial customers can manage Surface Duo 2 using any of the various enterprise mobility management (EMM) solutions that provide a consistent set of cloud-based device management capabilities whether managing employee- or company-owned devices.

Duo can be managed via the Microsoft EMM that uses a unified console, Microsoft Endpoint Manager, and extensible components such as Microsoft Intune. Alternatively, any EMM provider in Google's Android ecosystem can be used. In some cases, third-party EMM solutions

provide additional support to meet specific scenarios that may be useful depending on the environment.

To compare EMM solutions, refer to the Android Enterprise Solutions Directory. Endpoint Manager with Intune allows the user to manage Duo with the latest mobile device management policies as well as earlier technologies such as Exchange ActiveSync. If Exchange ActiveSync settings are already in use to manage mobile devices, those settings can be applied to Duo devices with Intune using an email device-configuration profile. For more information, refer to Add email settings to devices using Intune.

Because Intune is the primary means of managing devices, profiles provide default settings that can be customized to meet an organization's needs.

Table 2-1: Managing Personally Owned Surface Duo 2 Devices

Solution	Features	Learn More
App Protection Policies without device enrollment	Allows the user to manage and protect an organization's data within an application using deploy app protection policies, a lightweight management solution, without requiring device enrollment. A growing number of apps can be managed with app protection policies, including Microsoft Office and such third-party apps as Adobe Acrobat, Service Now, and Zoom.	Intune App Protection Policies overview
Android work profiles	Targeted at BYOD deployments, work profiles provide a separate space on Duo for work apps and data, giving organizations full control of their data, apps, and security policies without restricting users from using their device for personal apps and data.	Android work profiles

Table 2-2: Managing Corporate-Owned Surface Duo 2 Devices

Solution	Features	Learn more
Corporate-owned devices with work profile	Targeted at organizations that want to enable personal use on corporate-owned single-user devices that have been provided for work. This is designed to give organizations more granular control than managing with a work profile without completely locking down devices using full device management or dedicated device management.	Corporate-owned devices with work profile

Solution	Features	Learn more
	Work and personal profile app data is isolated by Android OS but differs from Android Enterprise work profile by providing admins more device-level control. IT admins can view, control, and configure the work accounts, applications, and data in the work profile, while end users are guaranteed that admins will have no visibility into the data and applications in the personal profile.	
Android Enterprise Fully Managed	Provides comprehensive device and app management capabilities for company-owned devices associated with a single user and leveraged exclusively for work and not personal use. Full device management provides IT with full control over device data and security, as well as access to Android's full suite of app management features. For example, the user also has full control over the apps on a device, including the ability to remotely install and remove apps.	Android Enterprise Fully Managed
Dedicated device management	This enterprise deployment scenario is targeted for devices deployed into specific use cases such as logistics, transportation, and factory floors. It is used for locked-down experiences in which the user needs to restrict usage to one or two apps and prohibit users from altering any settings.	Company owned devices for dedicated use

2.4 Surface Duo 2 Security Overview

Surface Duo 2 has built-in protection at every layer with deeply integrated hardware, firmware, and software to secure devices, identities, and data. As an Android 11 device, Surface Duo 2 uses Android security features at the operating system level and the Google services layer. The Android operating system leverages traditional operating system security controls to protect user data and system resources, protects device integrity against malware, and provides application isolation. Google also provides various services layered on top of the operating system that,

when combined with Android operating system security, help continuously protect the Android user.

- **Verified Boot:** Starting at the hardware level upon sign-in, Verified Boot strives to ensure executed code comes only from a trusted source. It establishes a full chain of trust from the hardware-protected root of trust to the bootloader, boot partition, and other verified partitions. When Surface Duo 2 boots up, each stage verifies the integrity and authenticity of the next stage before handing over execution.
- **App separation:** Application sandboxing isolates and guards Android apps, preventing malicious apps from accessing private information. Mandatory, always-on encryption and key handling help protect data in transit and at rest, even if devices fall into the wrong hands. Encryption is protected with Keystore keys, which store cryptographic keys in a container, making it more difficult to extract from a device.
- **Google Play Protect:** At the software layer, Surface Duo 2 uses Google Play Protect threat detection, which scans all applications, including public apps from Google Play, system apps updated by Microsoft and carriers, and sideloaded apps.

2.4.1 Mobile Device Management Security

Surface Duo 2 is secured in a corporate environment using an EMM solution that provides a consistent set of protection tools, technologies, and best practices that can be tailored to meet organizational and compliance requirements. A broad range of management APIs gives IT departments the tools to help prevent data leakage and enforce compliance in various scenarios. Multiprofile support and device management options enable the separation of work and personal data, helping keep company data secure.

MDM security is built on an expanding set of configuration technologies to enable users to be productive on the go while also protecting critical organization intellectual property. This includes app protection policies, device restriction policies, and related technologies designed to enable the organization to meet specific goals depending on the environment.

For example, device authentication can be strengthened by requiring a six-digit alphanumeric pin be entered, along with two-factor authentication. The devices to which users can enroll can be restricted to help ensure compliance with licensing limits or avoid granting access to "jailbroken" phones or other unsupported device types. Intune and other EMMs allow organizations to manage devices according to their needs.

2.4.2 Surface Duo 2 NIAP MDFPP and Commercial Solutions for Classified (CSfC) Compliance

Surface Duo 2 running Android 11 is compliant with NIAP-approved Protection Profile for Mobile Device Fundamentals version 3.1. Evaluation was carried out in accordance with the NIAP Common Criteria. (See Surface Duo 2 NIAP Certificate.)

The CSfC Program provides the ability to securely communicate based on commercial standards, protocols, algorithms, and modes to meet stringent NSA directives for classified information in solutions, ensuring users are equipped with devices at the cutting edge. This includes:

- Hardened device.
- Protecting data-at-rest and in transit.
- Controlling, managing, and enforcing mobile security policies.

Surface Duo 2 using Android 11 is currently certified for NIAP Mobile Device Fundamentals and will soon be in process for CSfC.

Table 2-3: Microsoft Surface Duo 2 NIAP Compliance

Product	Carrier	OS Version	Kernel	Build Number	WFA Cert #
Microsoft Surface Duo 2	Unlocked	Android 11	5.4.86	2022.110.15	WFA112939

2.4.3 Surface Duo 2 Auditing and Logging

Security and operational event logging is done by the operating system and applications to produce retrievable audit trails for troubleshooting, security monitoring, and forensics.

Surface Duo 2 leverages the standard Android logging mechanism to record the auditable events to help monitor security-related objectives. For this purpose, Android logs are configured to record each audit record, including date and time of events, type of event, subject identity, and outcome of the event. Thus, the integrity of audit logs must be protected from modification. This protection is achieved by SELinux policy and DAC.

Surface Duo 2 logging methods are described below:

- **Security Logs:** A table that depicts the list of all auditable events can be found here: https://developer.android.com/reference/android/app/admin/SecurityLog. The following link provides the additional information that can be grabbed when an MDM requests a copy of the logs: https://developer.android.com/reference/android/app/admin/SecurityLog.SecurityEvent. Each log contains a keyword or phrase describing the event, the date and time of the event, and further event-specific values that provide success, failure, and other information relevant to the event.
  - These logs can be read by an administrator via an MDM agent.
- **Logcat Logs:** Similar to Security Logs, Logcat Logs contain date, time, and specific values within the logs. They also provide a value mapped to a user ID to identify which user caused the event that generated the log. Logcat Logs tend to be more human-readable than Security Logs and are descriptive, not requiring the user to know the template of the log or code values to understand its reported values.
  - Logcat Logs can be configured to be exported to SD card and can always be viewed via an ADB shell to the device.
  - For the Logcat Logs, logging policy can be configured by MDM: Level of audit, log size, and list of logs to be recorded.