HONEYWELL ANDROID 9.X SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 1

14 January 2020

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

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

1.1 Executive Summary

The Honeywell Android 9.x Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to Honeywell Mobility Edge handheld devices running Android Pie (9) that process, store, or transmit unclassified data marked as "Controlled Unclassified Information (CUI)" or below.

This STIG leverages the Google Android 9.x STIG. All requirements in this STIG are based on the Google Android 9.x STIG with several Honeywell specific changes.

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

Note: This STIG requires that a NIAP-approved version of Android 9 be installed on DoD-owned Honeywell Android Mobility Edge devices. See the STIG requirement HONW-09-010900 for more information.

This STIG assumes that if a DoD Wi-Fi network allows a Honeywell Mobility Edge 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

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] Work data/apps only – no personal data/apps.
[2] 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 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 both at the device hardening level as well as at 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) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. HONEYWELL RUGGEDIZED ANDROID DEVICES

2.1 Honeywell Mobility Edge Mobile Computers Overview

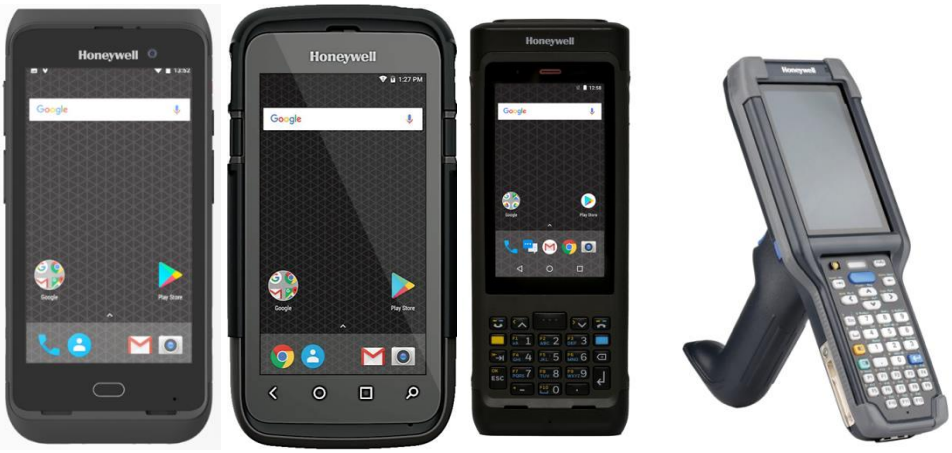
The Honeywell Mobility Edge platform devices are rugged and ultra-rugged Android 9 mobile computers for logistics, warehouse, and field mobility solutions. These Honeywell mobility edge devices are primarily used by (but not limited to) United States government agencies, government contractors, and businesses working with federal agencies.

These devices can be configured during initial deployment for either the COBO use case (also called Device Owner) or the COPE use case (Profile Owner). Depending on which use case is needed, users will deploy either the COPE or the COBO STIG supporting documentation and implementation guides.

Honeywell mobile devices all come with integrated short- and long-range scanners and removable batteries; are rugged devices with validated drop ratings; and have a wide range of accessories including scan handles, protective boots, CAC reader, and much more.

Figure 2-1: Honeywell Mobility Edge Devices

Devices shown, left to right are the Honeywell CT40, Honeywell CT60, Honeywell CN80, and Honeywell CK65.



2.2 Honeywell Mobile Computers Android Enterprise Compliance

Honeywell mobile computers are fully compliant with GMS (Google Mobile Services) and are also offered with an AOSP (non-GMS) operation system build. Both versions of the NIAP validated operating system can be downloaded from https://hsmftp.honeywell.com/. COBO devices are often used in a “single-use” application or environment where an organization may want to avoid GMS bundled applications and services that may not be required for their workflows. Honeywell Mobile computers using Android 9 are certified as Android Enterprise Recommended (AER) rugged devices. This implies that any mobile device management (MDM) system can be used on Honeywell mobile computers.

Honeywell Mobility Edge 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 user documentation as well as Google Android documentation.

2.3 Honeywell Mobility Edge Enterprise Work Profile Support

The enterprise program enables the administrator to define a work profile on the device. Fully managed devices with work profiles are for company-owned 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:

- Stronger set of policies for the work profile that apply to all work apps and data
- More lightweight set of policies for the personal profile that apply to the user's personal apps and data

Honeywell Mobility Edge devices support enterprise profiles to provide separation between private user applications and work (enterprise) applications, including the separation of private and enterprise applications' data. Applications installed into the enterprise versus personal profiles cannot access each other's secure data and applications and can have separate device administrators/managers. This functionality is built into the device by default and does not require an application download.

2.4 Honeywell Mobile Computers and NIAP Compliance

Honeywell mobile computers are compliant with NIAP-approved Protection Profile for Mobile Device Fundamentals. Evaluation was carried out in accordance with the NIAP Common Criteria. (See https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11002.)

Figure 2-2: Honeywell Mobile Computers with NIAP Compliance

Product	Model #	CPU	Kernel	Android OS version	Security Patch Level
CN80G	CN80-L1N	SDM660	4.4.153	Android 9.0	June, 2020
CN80G	CN80-L0N	SDM660	4.4.153	Android 9.0	June, 2020
CK65	CK65-L0N	SDM660	4.4.153	Android 9.0	June, 2020
CT60	CT60-L0N	SDM660	4.4.153	Android 9.0	June, 2020
CT60	CT60-L1N	SDM660	4.4.153	Android 9.0	June, 2020
CT40	CT40P-L0N	SDM660	4.4.153	Android 9.0	June, 2020
CT40	CT40P-L1N	SDM660	4.4.153	Android 9.0	June, 2020

2.5 Auditing and Logging

Audit and event logging is done by the underlying operating system and applications to produce retrievable log data for troubleshooting, security monitoring, and investigation forensics.

Honeywell Mobility Edge devices leverage the standard Android logging mechanism to record auditable events to help monitor security-related events. For this purpose, Android logs are configured to record each audit record, including event date and time, type, subject identity, and outcome. Thus, the integrity of audit logs must be protected from modification. This protection is achieved by the SELinux policy and dynamic access control.

Honeywell Mobility Edge device logging methods are described below:

- **Security Logs:** A table that depicts the list of all auditable events can be found at https://developer.android.com/reference/android/app/admin/SecurityLog. Device administrators can retrieve logging from the device using an MDM utility by following the instructions at: 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.
- **Application logging using intents and logcat:** Relevant logging can also be captured directly on the device using either Logcat or "Intents" provided by the application directly and do not require additional configuration or MDM utilities to be used.

2.6 Honeywell Enterprise Provisioner PPs That Mirror MDM STIG Configuration

Honeywell customers purchasing a Mobility Edge device also have the ability to configure and set the baseline of these devices using Honeywell Enterprise Provisioner in place of a regular MDM. The utility can be downloaded from https://www.honeywellaidc.com/resources/support. The protection profiles for Enterprise Provisioner that mirror MDM STIG configuration can also be downloaded from https://www.honeywellaidc.com/resources/support. The preferred approach continues to be a standard MDM utility, and EZConfig should only be used with the approval of the AO.

2.7 Honeywell CAC Reader

To support environments that may still require the use of a CAC, Honeywell Mobility edge devices support both Bluetooth CAC readers and USB snap-on (based on the model number).