IBM MaaS360 WITH WATSON V10.X MDM SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 2

26 April 2019

Developed by IBM 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

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The IBM MaaS360 with Watson v10.x Mobile Device Management (MDM) Security Technical Implementation Guide (STIG) provides security policy and configuration requirements for the use of the MaaS360 MDM software as a Service Enterprise Mobility Management platform to provide administrative management of Mobile Operating System (MOS) devices in the Department of Defense (DoD). This STIG applies to version 10.x of the MaaS360 server.

The MaaS360 product is deployed as a Software as a Service (SaaS) platform, where the server is installed in an IBM-controlled data center. The Supplemental document contains information regarding features, functions, and required Information Assurance (IA) controls for the implementation.

The scope of this STIG includes the Apple iOS 12 and the Samsung Android 8 devices. Several Samsung Android 8 STIG controls cannot be managed by the MaaS360 with Watson v10.x MDM. AOs can contact DISA at disa.stig_spt@mail.mil to obtain current information regarding the capability of the MaaS360 to manage STIG-required MDM controls for mobile devices.

1.1.1 Cloud Certification Information

Data stored on an MDM server, when deployed as a SaaS, includes the following:

- Device/User Information
    - Email address
    - Network domain user account is assigned to
    - Current status of user (for example, Active, Not Active)
    - Security policy assigned to device
    - List of device; model number; device ID; OS version; enrollment date; carrier name and network type; MAC address of the cellular, Bluetooth, and Wi-Fi ports
    - Compliance status of user's device
    - List of apps installed on device
- List of all mobile device security policies used in the organization
    - List of each control setting enforced by the policy
    - List of every device the MDM security policy is assigned to
- List of applications managed by the MDM

DoD Approving Authorities should determine the appropriate information Impact Level (IL) for an MDM SaaS deployment based on their operational environment in accordance with (IAW) the Cloud Computing Security Requirements Guide (SRG). DISA's recommendation is that IL 4 or 5 is appropriate for most DoD environments.

The MaaS360 SaaS platform has completed Federal Risk and Authorization Management Program (FedRAMP) certification (Level 2 Provisional Authorization [PA]).

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 Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.mil/.

1.5 MDMPP Compliance Reporting

All Mobile Device Management Protection Profile (MDMPP) 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 MDMPP.

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) (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