National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Extended Package for Mobile Device Management Agents, Version 2.0, December 31st, 2014

Report Number: CCEVS-VR-PP-0030
Dated: 24 June 2016
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Base and Additional Requirements
Gossamer Security Solutions
Catonsville, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Extended Package for Mobile Device Management Agents, Version 2.0 (MDMAEP20). It presents a summary of the MDMAEP20 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the MDMAEP20 was performed concurrent with the first product evaluation against the EP's requirements. In this case the Target of Evaluation (TOE) for this first product was the MobileIron Mobile@Work for Android, version 8.6. The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in June 2016. This evaluation addressed the base requirements of the MDMAEP.

The information in this report is largely derived from the Evaluation Technical Report (ETR) and Assurance Activity Report (AAR), each written by the Gossamer CCTL.

The evaluation determined that the MDMAEP20 is both Common Criteria Part 2 Extended and Part 3 Conformant. The EP identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). The Security Target (ST) contains material drawn directly from the MDMAEP20 as well as the Protection Profile for Mobile Device Management, which is assessed in a separate Validation Report. Performance of the majority of the ASE work units serves to satisfy the APE work units as well for both the claimed PP and the claimed EP. Where this is not the case, the lab performed the outlying APE work units as part of this evaluation.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team found that the evaluation showed that the MDMAEP20 meets the requirements of the APE components. The conclusions of the testing laboratory in the assurance activity report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profiles containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of the MDMAEP20 was performed concurrent with the first product evaluation against the PP. In this case the TOE for this first product was the MobileIron Mobile@Work for Android component of the MobileIron Platform, Version 9.0, developed by MobileIron, Inc. The evaluation was performed by the

Gossamer Security Solutions Common Criteria Testing Laboratory (CCTL) in Catonsville, Maryland, United States of America, and was completed in June 2016.

The MDMAEP20 contains a set of "base" requirements that all conformant STs must include and "additional" requirements that may or may not apply to a conformant TOE depending on its architecture and intended usage.

Because these optional requirements may not be included in a particular ST, the initial use of the EP will address (in terms of the EP evaluation) the base requirements as well as any additional requirements that are incorporated into that initial ST. Subsequently, TOEs that are evaluated against the MDMAEP20 that incorporate additional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and any appropriate updates to this validation report will be made.

The following identifies the EP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this EP, as well as subsequent evaluations that address additional optional requirements in the MDMAEP20.

Protection Profile	*Extended Package for Mobile Device Management Agents, Version 2.0*
ST (Base)	MobileIron Platform (MDMAEP20 and MDMAEP20) Security Target, Version 1.0
Assurance Activity Report (Base)	Assurance Activity Report (MDMAEP20 and MDMAEP20) for MobileIron Platform, Version 0.3
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
CCTL (base)	Gossamer Security Solutions, Catonsville, MD USA
CCEVS Validators (base)	Kenneth Elliott, Aerospace Corporation
	Meredith Hennan, Aerospace Corporation
	Luke Florer, Aerospace Corporation
	Jerome Myers, Aerospace Corporation
	Kenneth Stutterheim, Aerospace Corporation
	Sheldon Durrant, MITRE Corporation

3 MDMAEP Description

Mobile device management (MDM) products allow enterprises to apply security policies to mobile devices, such as smartphones and tablets. The purpose of these policies is to establish a security posture adequate to permit mobile devices to process enterprise data and connect to enterprise network resources.

The MDMAEP provides a baseline set of Security Functional Requirements (SFRs) for an MDM Agent, which is the Target of Evaluation (TOE). The MDM Agent is only one component of an enterprise deployment of mobile devices. Other components, such as the mobile device platforms, which enforce the security policies, and network access control

servers, are out of scope. The MDMAEP exists as an extended package (EP) of both the Protection Profile for Mobile Device Fundamentals and the Protection Profile for Mobile Device Management. This means that a TOE that claims conformance to either of these PPs may opt to claim this EP if it provides MDM Agent functionality. This EP does not exist as a standalone PP; instead, the evaluation methods and Security Assurance Requirements (SARs) that are performed by the evaluator against the "base" PP are extended to apply to the security functionality addressed by this EP.

The MDM Agent is installed on a mobile device as an application or is part of the mobile device's OS. The MDM Agent establishes a secure connection back to the MDM Server controlled by an enterprise administrator. Optionally, the MDM Agent interacts with the Mobile Application Store (MAS) Server to download and install enterprise-hosted application.

The MDM Agent must closely interact with or be part of (as depicted by the dotted red/blue line in Figure 1) the mobile device's platform to establish policies and perform queries about device status. The mobile device, in turn, has its own security requirements specified in the MDF PP against which the mobile device must be evaluated either concurrently with or before the MDM Agent evaluation.

If the MDM Agent is part of the mobile device's OS, the agent may present multiple interfaces for configuring the mobile device, such as a local interface and a remote interface. Agents conforming to the MDMAEP must at least offer an interface with a trusted channel that serves as one piece of an MDM system. Compliant agents may also offer other interfaces, and the configuration aspects of these additional interfaces is in scope of this EP.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: TOE Assumptions

Assumption Name	Assumption Definition
A.CONNECTIVITY	The TOE relies on network connectivity to carry out its management activities. The TOE will robustly handle instances when connectivity is unavailable or unreliable.
A.MOBILE_DEVICE_PLATFORM	The MDM Agent relies upon Mobile platform and hardware evaluated against the MDFPP and assured to provide policy enforcement as well as cryptographic services and data protection. The Mobile platform provides trusted updates and software integrity verification of the MDM Agent.
A.PROPER_ADMIN	One or more competent, trusted personnel who are not careless, willfully negligent, or hostile, are assigned and authorized as the TOE Administrators, and do so using and abiding by guidance documentation.
A.PROPER_USER	Mobile device users are not willfully negligent or hostile, and use the device within compliance of a reasonable Enterprise security policy

4.2 Threats

Table 2: Threats

Threat Name	Threat Definition
T.MALICIOUS_APPS	An administrator of the MDM or mobile device user may inadvertently import malicious code, or an attacker may insert malicious code into the TOE or OE, resulting in the compromise of TOE or TOE data
T.NETWORK_ATTACK	An attacker may masquerade as MDM Server and attempt to compromise the integrity of the mobile device by sending malicious management commands.
T.NETWORK_EAVESDROP	Unauthorized entities may intercept communications between the MDM and mobile devices to monitor, gain access to, disclose, or alter remote management commands. Unauthorized entities may intercept unprotected wireless communications between the mobile device and the Enterprise to monitor, gain access to, disclose, or alter TOE data.
T.PHYSICAL_ACCESS	The mobile device may be lost or stolen, and an unauthorized individual may attempt to access OE data.

4.3 Organizational Security Policies

Table 3: Threats

OSP Name	OSP Definition
P.ADMIN	The configuration of the mobile device security functions must adhere to the Enterprise security policy.
P.DEVICE_ENROLL	A mobile device must be enrolled for a specific user by the administrator of the MDM prior to being used in the Enterprise network by the user.
P.NOTIFY	The mobile user must immediately notify the administrator if a mobile device is lost or stolen so that the administrator may apply remediation actions via the MDM system.
P.ACCOUNTABILITY	Personnel operating the TOE shall be accountable for their actions within the TOE.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 4: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.APPLY_POLICY	The TOE must facilitate configuration and enforcement of enterprise security policies on mobile devices via interaction with the MDM Agent. This will include the initial enrollment of the device into management, through its lifecycle including policy updates and through its possible unenrollment from management services

TOE Security Obj.	TOE Security Objective Definition
O.ACCOUNTABILITY	The TOE must provide logging facilities which record management actions undertaken by its administrators.
O.DATA_PROTECTION_TRANSIT	Data exchanged between the MDM Server and the MDM Agent and between the MDM Server and its operating environment must be protected from being monitored, accessed and altered.

The following table contains objectives for the Operational Environment.

Table 5: Security Objectives for the Operational Environment

Environmental Security Obj.	TOE Security Objective Definition
OE.IT_ENTERPRISE	The Enterprise IT infrastructure provides security for a network that is available to the TOE and mobile devices that prevents unauthorized access
OE.MOBILE_DEVICE_PLATFORM	The MDM Agent relies upon the trustworthy Mobile platform and hardware to provide policy enforcement as well as cryptographic services and data protection. The Mobile platform provides trusted updates and software integrity verification of the MDM Agent.
OE.PROPER_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner
OE.PROPER_USER	Users of the mobile device are trained to securely use the mobile device and apply all guidance in a trusted manner.
OE.WIRELESS_NETWORK	A wireless network will be available to the mobile devices.

5 Requirements

As indicated above, requirements in the MDMAEP20 are comprised of the "base" requirements and additional requirements that are conditionally or strictly optional. The following table contains the "base" requirements that were validated as part of the evaluation activity referenced above.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_ALT_EXT.2: Agent Alerts
FIA: Identification and Authentication	FIA_ENR_EXT.2: Enrollment of Mobile Device into Management
FMT: Security Management	FMT_SMF_EXT.3: Specification of Management Functions
	FMT_UNR_EXT.1: User Unenrollment Prevention

The following table contains the optional requirements contained in the appendices of MDMAEP20 and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST. This table includes all optional requirements, whether they are strictly optional or conditionally optional (e.g. selection-based), and whether they must be implemented by the TOE or can be implemented by the underlying platform.

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1(2): Audit Data Generation	
	FAU_SEL.1(2): Security Audit Event Selection	
	FAU_STG_EXT.1: Security Audit Event Storage	
FMT: Security Management	FMT_POL_EXT.2: Trusted Policy Update	

6 Assurance Requirements

The MDMAEP20 defines no assurance requirements. The functionality defined in the MDMAEP20 is evaluated by applying the same assurance requirements that are defined in the "base" PP to the entire TOE (i.e. the portion that is addressed by the base PP as well as the portion that is addressed by this EP).

7 Results of the Evaluation

The CCTL produced an ETR that contained the following results. Note that for APE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

APE Requirement	Evaluation Verdict
APE_CCL.1	Pass
APE_ECD.1	Pass
APE_INT.1	Pass
APE_OBJ.2	Pass
APE_REQ.1	Pass – note as per section 6, this EP deliberately excludes assurance requirements so this part of APE_REQ.1 was N/A

8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance in the Assurance Activities to determine whether or not the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.

- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 4, dated: September 2012.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 4, dated: September 2012.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 4, dated: September 2012.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 4, dated: September 2012.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Gossamer Security Solutions, *MobileIron Platform (MDMAEP20 and MDMAEP20) Security Target*, Version 1.0, May 27, 2016.

[7] Gossamer Security Solutions, *Assurance Activity Report (MDMAEP20/MDMAEP20) for MobileIron Platform*, Version 0.3, May 27, 2016.

[8] Extended Package for Mobile Device Management Agents, Version 2.0, December 31, 2014.