National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Protection Profile for Mobile Device Management

Version 3.0

21 November 2016

Report Number: CCEVS-VR-PP-0053
Dated: 09 September 2019
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 Protection Profile for Mobile Device Management, Version 3.0 (PP_MDM_V3.0). It presents a summary of the PP_MDM_V3.0 and the evaluation results.

Gossamer Security Solutions, located in Catonsville, Maryland, performed the evaluation of PP_MDM_V3.0 concurrent with the first product evaluation against the PP's requirements. The evaluated product was MobileIron Platform version 10.

This evaluation addressed the base requirements of PP_MDM_V3.0 and several of the additional requirements contained in Appendices A, B and C.

The Validation Report (VR) author independently performed an additional review of the PP as part of the completion of this VR, to confirm it meets the claimed APE assurance requirements.

The evaluation determined that PP_MDM_V3.0 is both Common Criteria Part 2 Extended and Part 3 Conformant. The PP identified in this VR has been evaluated at NIAP approved CCTLs 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) includes material from both the PP_MDM_V3.0 and the MDM Agent Extended Package; completion of the ASE work units satisfied the APE work units for PP_MDM_V3.0, but only for those parts of the Security Target that were relevant to this PP.

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

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 CCTLs. CCTLs evaluate products against PPs that contain Evaluation 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 PP_MDM_V3.0 was performed concurrent with the first product evaluation against the PP's requirements. In this case, the Target of Evaluation (TOE) was MobileIron Platform version 10, evaluated by Gossamer Security Solutions in Catonsville, Maryland, United States of America

These evaluations addressed the base requirements of PP_MDM_V3.0, and several of the additional requirements contained in Appendices A, B and C.

PP_MDM_V3.0 contains a set of "base" requirements that all conformant STs must include, and additionally contains "Optional", "Selection-based", and "Objective" requirements. Optional requirements may or may not be included within the scope of the evaluation, depending on whether the vendor provides that functionality within the tested product and

chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based upon the selections made in the base requirements and the capabilities of the TOE. Objective requirements specify optional functionality that the PP authors consider candidates for becoming mandatory requirements in the future.

A specific ST may not include all non-base requirements, so the initial use of the PP addresses (in terms of the PP evaluation) the base requirements and any additional requirements incorporated into the initial ST. The VR authors have evaluated all discretionary requirements that were not claimed in the initial TOE evaluation as part of the evaluation of the APE_REQ workunits performed against PP_MDM_V3.0. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include reference to this as additional evidence that the corresponding portions of PP_MDM_V3.0 were evaluated.

The following identifies the PP subject of the evaluation/validation, as well as the supporting information from the evaluation performed against this PP and any subsequent evaluations that address additional optional and/or selection-based requirements in the PP_MDM_V3.0.

Protection Profile	Protection Profile for Mobile Device Management, Version 3.0, 21 November 2016.
ST (Base)	MobileIron Platform (MDMPP30 and MDMAEP30) Security Target, Version 0.8, 04 January 2019
Assurance Activity Report (Base)	Assurance Activity Report (MDMPP/MDMAEP30) for Mobile Iron Platform, Version 0.2, 08 January 2019
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 4
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CCTLs	Gossamer Security Solutions, Catonsville, Maryland

3 PP_MDM_V3.0 Description

The PP_MDM_V3.0 specifies information security requirements for mobile device management, as well as the assumptions, threats, organizational security policies, objectives, and requirements of a compliant TOE.

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.

This Protection Profile (PP) describes security requirements for an MDM System, which is the Target of Evaluation (TOE). The MDM System is only one component of an enterprise deployment of mobile devices.

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: 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.MDM_SERVER_PLATFORM	The MDM Server relies upon a trustworthy platform and local network from which it provides administrative capabilities. The MDM server relies on the this platform to provide a range of security-related services including reliable timestamps, user and group account management, logon and logout services via a local or network directory service, remote access control, and audit log management services to include offloading of audit logs to other servers. The platform is expected to be configured specifically to provide MDM services, employing features such as a host-based firewall, which limits its network role to providing MDM functionality.
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

The following table contains applicable threats.

Table 2: Threats

Threat Name	Threat Definition
T.MALICIOUS_APPS	Malicious or flawed application threats exist because apps loaded onto a mobile device may include malicious or exploitable code. An administrator of the MDM or mobile device user may inadvertently import malicious code, or an attacker may insert malicious code into the TOE, 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 user data. Although these attacks are primarily directed against the mobile device platform, the TOE configures features, which address these threats.

4.3 Organizational Security Policies

The following table contains applicable organizational security policies.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
P.ACCOUNTABILITY	Personnel operating the TOE shall be accountable for their actions within the TOE.
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.

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.ACCOUNTABILITY	The TOE must provide logging facilities which record management actions undertaken by its administrators.
O.APPLY_POLICY	The TOE must facilitate configuration and enforcement of enterprise security policies on mobile devices via interaction with the mobile OS and the MDM Server. This will include the initial enrollment of the device into management through its entire lifecycle, including policy updates and its possible unenrollment from management services.
O.DATA_PROTECTION_TRANSIT	Data exchanged between the MDM Server and the MDM Agent must be protected from being monitored, accessed, or altered.
O.INTEGRITY	The TOE will provide the capability to perform self-tests to ensure the integrity of critical functionality, software/firmware and data has been maintained. The TOE will also provide a means to verify the integrity of downloaded updates.
O.MANAGEMENT	The TOE provides access controls around its management functionality.

The following table contains security objectives for the Operational Environment.

Table 5: Security Objectives for the Operational Environment

Environmental Security Obj.	Environmental Security Objective Definition
OE.DATA_PROPER_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
OE.DATA_PROPER_USER	Users of the mobile device are trained to securely use the mobile device and apply all guidance in a trusted manner.
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.TIMESTAMP	Reliable timestamp is provided by the operational environment for the TOE.
OE.WIRELESS_NETWORK	A wireless network will be available to the mobile devices.

5 Requirements

As indicated above, requirements in the PP_MDM_V3.0 are comprised of the "base" requirements and additional requirements that are optional, selection-based, or objective. The following table contains the "base" requirements that were validated as part of the MobileIron evaluation activities referenced above.

Table 6: Base Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_ALT_EXT.1: Server Alerts	MobileIron Platform version 10
	FAU_NET_EXT.1: Network Reachability Review	MobileIron Platform version 10
FIA: Identification and Authentication	FIA_ENR_EXT.1: Enrollment of Mobile Device into Management	MobileIron Platform version 10
FMT: Security Management	FMT_MOF.1(1): Management of Functions Behavior	MobileIron Platform version 10
	FMT_MOF.1(2): Management of Functions Behavior (Enrollment)	MobileIron Platform version 10
	FMT_POL_EXT.1: Trusted Policy Update	MobileIron Platform version 10
	FMT_SMF.1(1) Specification of Management Functions (Server configuration of Agent)	MobileIron Platform version 10
	FMT_SMF.1(2) Specification of Management Functions (Server Configuration of Server)	MobileIron Platform version 10
	FMT_SMR.1(1) Security Management Roles	MobileIron Platform version 10
FPT: Protection of the TSF	FPT_TUD_EXT.1: Trusted Update	MobileIron Platform version 10

Note that the PP also defines two SFRs, FPT_ITT.1 and FTP_ITC.1(2), such that at least one of them must be required depending on how the TOE is deployed. FPT_ITT.1 must be claimed if the TOE includes an MDM agent, whereas FTP_ITC.1(2) must be claimed if the TOE interoperates with an MDM agent that is pre-deployed on a mobile device in its operational environment. The MobileIron evaluation includes its own MDM agent so

FPT_ITT.1 was claimed. Both of these SFRs are listed as optional requirements in Table 8 below.

The following table lists functionality that must be implemented either by a conformant TOE or by the TOE's invocation of functions in its Operational Environment. If no completed evaluations have claimed a requirement as being implemented by the TSF, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "PP Evaluation".

Table 7 TOE or Platform Security Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1(1): Audit Data Generation	MobileIron Platform version 10
	FAU_STG_EXT.1(1): External Trail Storage	MobileIron Platform version 10
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation:	MobileIron Platform version 10
	FCS_CKM.2: Cryptographic Key Establishment	MobileIron Platform version 10
	FCS_CKM_EXT.4: Cryptographic Key Destruction	MobileIron Platform version 10
	FCS_COP.1(1): Cryptographic Operation (Confidentiality Algorithms)	MobileIron Platform version 10
	FCS_COP.1(2): Cryptographic Operation (Hashing Algorithms)	MobileIron Platform version 10
	FCS_COP.1(3): Cryptographic Operation (Signature Algorithms)	MobileIron Platform version 10
	FCS_COP.1(4): Cryptographic Operation (Keyed-Hash Message Authentication)	MobileIron Platform version 10
	FCS_RBG_EXT.1: Random Bit Generation	MobileIron Platform version 10
	FCS_STG_EXT.1: Cryptographic Key Storage	MobileIron Platform version 10
FIA: Identification and Authentication	FIA_UAU.1: Timing of Authentication	MobileIron Platform version 10
	FIA_X509_EXT.1: Validation of Certificates	MobileIron Platform version 10
	FIA_X509_EXT.2: X.509 Certificate Authentication	MobileIron Platform version 10
FPT: Protection of the TSF	FPT_TST_EXT.1: TSF Functionality Testing	MobileIron Platform version 10
	FPT_TUD_EXT.1: Trusted Update	MobileIron Platform version 10
FTP: Trusted Path/Channels	FTP_ITC.1(1): Inter-TSF Trusted Channel (Authorized IT Entities)	MobileIron Platform version 10
	FTP_TRP.1(1): Trusted Path (Remote Administration)	MobileIron Platform version 10
	FTP_TRP.1(2): Trusted Path (for Enrollment)	MobileIron Platform version 10

The following table contains the "**Optional**" requirements contained in Appendix A, and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given optional requirement, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "PP Evaluation".

Table 8: Optional Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1(2): Audit Generation (MAS Server)	MobileIron Platform version 10
	FAU_SAR.1: Audit Review	MobileIron Platform version 10
	FAU_SEL.1: Security Audit Event Selection	
	FAU_STG_EXT.1(2): External Audit Trail Storage (MAS Server)	PP Evaluation
FCS: Cryptographic Support	FCS_TLSC_EXT.1: TLS Client Protocol	MobileIron Platform version 10
FMT: Security Management	FMT_MOF.1(3): Management of Functions (MAS Server)	MobileIron Platform version 10
	FMT_MOF.1(4): Management of Functions (MAS Server Downloads)	MobileIron Platform version 10
	FMT_SMF.1(3): Specification of Functions (MAS Server)	MobileIron Platform version 10
	FMT_SMR.1(2): Security Management Roles (MAS Server)	PP Evaluation
FPT: Protection of the TSF	FPT_ITT.1: Internal TOE TSF Data Transfer	MobileIron Platform version 10
FTA: TOE Access	FTA_TAB.1: TOE Access Banner	MobileIron Platform version 10
FTP: Trusted Path/Channels	FTP_ITC.1(2): Inter-TSF Trusted Channel (MDM Agent)	MobileIron Platform version 10
	FTP_ITC.1(3): Inter-TSF Trusted Channel (MAS Server)	PP Evaluation

The following table contains the "**Selection-Based**" requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "PP Evaluation".

Table 9: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_STG_EXT.2: Audit Event Storage	MobileIron Platform version 10
FCS: Cryptographic Support	FCS_DTLS_EXT.1: DTLS Protocol	PP Evaluation
	FCS_HTTPS_EXT.1: HTTPS Protocol	MobileIron Platform version 10
	FCS_IV_EXT.1: Initialization Vector Generation	PP Evaluation
	FCS_STG_EXT.2: Encrypted Cryptographic Key Storage	PP Evaluation
	FCS_TLSC_EXT.1: TLS Client Protocol – Elliptic Curves Extension[1]	MobileIron Platform version 10

[1] FCS_TLSC_EXT.1 is an optional requirement in Appendix A. Appendix B contains one element, FCS_TLSC_EXT.1.5 that is conditionally applicable depending on the selections made in the Appendix A SFR.

	FCS_TLSS_EXT.1: TLS Server Protocol	MobileIron Platform version 10

The following table contains the "**Objective**" requirements contained in Appendix C, and an indication of what evaluation those requirements were verified in (from the list in the Identification section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "PP Evaluation".

Table 10: Objective Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_CRP_EXT.1: Support for Compliance Reporting of Mobile Device Configuration (FAU_CRP)	MobileIron Platform version 10
FCS: Cryptographic Support	FCS_TLSC_EXT.1: TLS Client Protocol (Signature Algorithms Extension)[2]	PP Evaluation
	FCS_TLSS_EXT.1: TLS Server Protocol (Signature Algorithms Extension)[3]	PP Evaluation
FIA: Identification and Authentication	FIA_UAU_EXT.4(1): User Authentication (Re-Use Prevention)	PP Evaluation
	FIA_UAU_EXT.4(2): User Authentication (Re-Use Prevention for Device Enrollment)	PP Evaluation
	FIA_X509_EXT.3: X.509 Enrollment	PP Evaluation
	FIA_X509_EXT.4: Alternate X.509 Enrollment	PP Evaluation
FMT: Security Management	FMT_SAE_EXT.1: Security Attribute Expiration	MobileIron Platform version 10

6 Assurance Requirements

The following are the assurance requirements contained in the PP_MDM_V3.0.

Table 11: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ASE: Security Target	ASE_CCL.1: Conformance Claims	MobileIron Platform version 10
	ASE_ECD.1: Extended Components Definition	MobileIron Platform version 10
	ASE_INT.1: ST Introduction	MobileIron Platform version 10
	ASE_OBJ.1: Security Objectives for the Operational Environment	MobileIron Platform version 10
	ASE_REQ.1: Stated Security Requirements	MobileIron Platform version 10
	ASE_SPD.1: Security Problem Definition	MobileIron Platform version 10
	ASE_TSS.1: TOE Summary Specification	MobileIron Platform version 10
ADV:	ADV_FSP.1 Basic Functional Specification	MobileIron Platform version 10

[2] FCS_TLSC_EXT.1 is an optional requirement in Appendix A. Appendix C contains three elements, FCS_TLSC_EXT.1.6 through 1.8 that are objective depending on the selections made in the Appendix A SFR.
[3] FCS_TLSS_EXT.1 is a selection-based requirement in Appendix B. Appendix C contains three elements, FCS_TLSS_EXT.1.7 through 1.9 that are objective depending on the selections made in the Appendix B SFR.

Development		
AGD: Guidance Documents	AGD_OPE.1: Operational User Guidance	MobileIron Platform version 10
	AGD_PRE.1: Preparative Procedures	MobileIron Platform version 10
ALC: Life-cycle Support	ALC_CMC.1: Labeling of the TOE	MobileIron Platform version 10
	ALC_CMS.1: TOE CM Coverage	MobileIron Platform version 10
ATE: Tests	ATE_IND.1: Independent Testing - Sample	MobileIron Platform version 10
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	MobileIron Platform version 10

7 Results of the Evaluation

Note that for APE elements and work units that are identical to ASE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

Table 12: Evaluation Results

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	MobileIron Platform version 10; PP evaluation
APE_ECD.1	Pass	MobileIron Platform version 10; PP evaluation
APE_INT.1	Pass	MobileIron Platform version 10; PP evaluation
APE_OBJ.1	Pass	MobileIron Platform version 10; PP evaluation
APE_REQ.1	Pass	MobileIron Platform version 10; PP evaluation
APE_SPD.1	Pass	MobileIron Platform version 10; PP evaluation

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 PP_MDM_V3.0 Evaluation 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.

- **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 VR:

[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*, 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 3.0, May 2014.

[6] Protection Profile for Mobile Device Management, Version 3.0, 21 November 2016.

[7] MobileIron Platform (MDMPP30 and MDMAEP30) Security Target, Version 0.8, 04 January 2018.

[8] Assurance Activity Report (MDMPP30/MDMAEP30) for MobileIron Platform, Version 0.2, 08 January 2019.