National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

MobileIron

415 East Middlefield Road

Mountain View, CA 94043

MobileIron Platform Version 9.0

Report Number: **CCEVS-VR-10584-2016**
Dated: **June 14, 2016**
Version: **0.1**

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

Validation Team

Kenneth Elliott
Meredith Hennan
Luke Florer
Jerome Myers
Kenneth Stutterheim
Aerospace Corporation

Sheldon Durrant
MITRE Corporation

Common Criteria Testing Laboratory

Cornelius Haley
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of MobileIron Platform solution provided by MobileIron It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

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. The information in this report is largely derived from the proprietary Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant.

The Target of Evaluation (TOE) is the MobileIron Platform Version 9.0. The product is composed of MobileIron Core and the MobileIron Client also known as Mobile@Work for Android, Version 8.6. The MobileIron Core defines security and management policies for mobile apps, content and devices independent of the mobile device operating system. MobileIron Client automatically configures the device to function in an enterprise environment by enforcing the configuration and security policies set by the IT department.

The Target of Evaluation (TOE) 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). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory’s findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the MobileIron Platform (MDMPP20/MDMAEP20) Security Target, Version 1.0, May 27, 2016 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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 Profile containing Assurance Activities that are interpretation of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP and in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	MobileIron Platform Version 9.0 (Specific models identified in Section 3.1)
Protection Profile	Protection Profile for Mobile Device Management, Version 2.0, 31 December 2014 (MDMPP20) Extended Package for Mobile Device Management Agents, Version 2.0, 31 December 2014 (MDMAEP20)
ST:	MobileIron Platform (MDMPP20/MDMAEP20) Security Target, Version 1.0, May 27, 2016
Evaluation Technical Report	Evaluation Technical Report for MobileIron Platform, Version 1.0, May 27, 2016.
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	MobileIron
Developer	MobileIron
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.

Item	Identifier
CCEVS Validators	Kenneth Elliott, Luke Florer, Meredith Hennan, Jerome Myers, Kenneth Stutterheim, The Aerospace Corporation Sheldon Durrant, MITRE Corporation

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Target of Evaluation (TOE) the MobileIron Core server and associated MobileIron Client (also referred to as Mobile@Work) agents for Android devices, both of which are part of their MobileIron Platform. Note that the MobileIron Platform consists of other components (MobileIron Sentry and additional mobile device applications, e.g., Web@work, Docs@work, AppConnect container and Secure Application Manager) that do not play a role in enforcing the security functions included in the MobileIron Platform (MDMPP20/MDMAEP20) Security Target and were not evaluated.

The TOE is an MDM solution where the claimed security functions are implemented in a central MDM server – MobileIron Core - and distributed MDM agents – MobileIron Client.

MobileIron Core (http://www.mobileiron.com/en/products/core) integrates with backend enterprise IT systems and enables IT to define security and management policies for mobile apps, content and devices independent of the operating system. MobileIron Core enables mobile device, application, and content management.

- Mobile device management capabilities are the primary focus of this evaluation and enable IT to securely manage mobile devices across mobile operating systems and provide secure corporate email, automatic device configuration, certificate-based security, and selective wiping of enterprise data from both corporate-owned as well as user-owned devices.
- Mobile application management capabilities are a secondary focus of this evaluation and help IT manage the entire application lifecycle, from making the applications available in the enterprise app storefront, facilitating deployment of applications to mobile devices, and retiring applications as necessary. Note that this capability is referred to as MAS – Mobile Application Store – Server in the Security Target.
- Mobile content management functions are included in the MobileIron Platform, but no claims are made about those capabilities in the Security Target.

MobileIron Client (http://www.mobileiron.com/en/products/client) – also known as Mobile@Work – is an app downloaded by end users onto their mobile devices. It automatically configures the device to function in an enterprise environment by enforcing the configuration and security policies set by the IT department. Once installed, it creates a secure MobileIron container to protect enterprise data and applications.

- The MobileIron Client works with MobileIron Core to configure corporate email, Wi-Fi, VPN, and security certificates and to create a clear separation between personal and business information. This allows IT to selectively wipe only the corporate data on the device if the user leaves the company, if the device falls out of compliance, or is lost.
- The MobileIron Client also enables additional enterprise device controls that are not subject to security claims and hence are outside the scope of the evaluation related to the Security Target.

3.1 TOE Architecture

MobileIron offers a MobileIron Platform solution comprised of MobileIron Core, MobileIron Sentry, MobileIron Client, and mobile end user products (e.g., smartphones).

Of these components, the TOE is a central MobileIron Core server and MobileIron Clients installed on distributed end user mobile Android devices. MobileIron Sentry is another security product not within scope of this evaluation (i.e., the MDMPP20 requirements are not applicable), but can freely be used with the TOE in its evaluated configuration.

3.2 Physical Boundaries

The TOE consists of two software components: MobileIron Core and MobileIron Client. MobileIron Core is a server that is deployed on a CentOS 6.7 Linux operating system (OS) that runs on an Intel x64 architecture server platform. MobileIron supports the MobileIron Core operating on one of three physical server appliances: Mobile Iron M2100, M2200, or M2500, as well as virtual deployments in VMWare ESXi (5.1, 5.5, or 6.0) and Microsoft Hyper-V (Server 2008 R2 or Server 2012 R2).

The Mobile Iron appliances are all based on Intel Xeon CPUs (E3-1200 or E5-2670) and utilize Intel network adapters (82579LM GbE, 82574L GbE, or Quad I350 GbE) along with SATA disk drives and DRAM from 32-64 GB. Virtual deployments must use a 64-bit x86 virtual machine and an E1000 network adapter. The vendor recommends at least 8 Gb RAM and 80 Gb storage.

MobileIron Client consists of apps deployed on Android mobile devices. There are a number of evaluated Samsung Galaxy mobile Android devices (including Galaxy S4, Galaxy Note 3, Galaxy S5, Galaxy Note 4, and Galaxy S6 models) ranging from Android version 4.4 to 5.0.2 that can be used with the Android version of the MobileIron Client.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security Management
5. Protection of the TSF

6. TOE access
7. Trusted path/channels

4.1 Security audit

The MDM Server can generate and store audit records for security-relevant events as they occur. These events are stored and protected by the MDM Server and can be reviewed by an authorized administrator. The MDM Server can be configured to export the audit records in either in CSV (comma separated values) format, text format, or a compressed archive format utilizing TLS for protection of the records on the network. The MDM Server also supports the ability to query information about MDM agents and export MDM configuration information.

The MDM Agent includes the ability to indicate (i.e., respond) when it has been enrolled and when policies are applied to the MDM Agent. The MDM Server can be configured to alert an administrator based on its configuration. For example, it can be configured to alert the administrator when a policy update fails or an MDM Agent has been enrolled.

4.2 Cryptographic support

The MDM Server and MDM Agent both include and/or utilize cryptographic modules or libraries with National Voluntary Laboratory Accreditation Program (NVLAP) Cryptographic Algorithm Validation Program (CAVP) validated algorithms for a wide range of cryptographic functions including: asymmetric key generation and establishment, encryption/decryption, cryptographic hashing and keyed-hash message authentication. These functions are supported with suitable random bit generation, initialization vector generation, secure key storage, and key and protected data destruction.

The primitive cryptographic functions are used to implement security communication protocols: TLS, HTTPS, and SSH used for communication between the MDM Server and MDM Agent and between the MDM Server and remote administrators.

4.3 Identification and authentication

The MDM Server requires mobile device users (MD users) and administrators to be authenticated prior to allowing any security-related functions to be performed. This includes MD users enrolling their device in the MDM Server using a corresponding MDM Agent as well as an administrator logging on to manage the MDM Server configuration, MDM policies for mobile devices, etc.

In addition, both the MDM Server and MDM Agent utilize X.509 certificates, including certificate validation checking, in conjunction with TLS to secure communications between the MDM Server and MDM Agents as well as between the MDM Server and administrators using a web-based user interface for remote administrative access.

4.4 Security management

The MDM Server is designed to include at least two distinct user roles: administrator and mobile device user (MD user). The former interacts directly with the MDM Server while the latter is the user of a mobile device hosting an MDM Agent. The MDM Server further supports the fine-grain assignment of role (access to management function) to defined users allowing the definition of multiple user and administrator roles with different capabilities and responsibilities.

The MDM Server provides the functionality necessary to manage its own security functions as well as to manage mobile device policies that are sent to MDM Agents. In addition, the MDM Server ensures that security management functions are limited to authorized administrators while allowing MD users to perform only necessary functions such as enrolling in the MDM Server.

The MDM Agents provide the functions necessary to securely communicate with and enroll in a MDM Server, implement policies received from and enrolled MDM Server, and report the results of applying policies.

4.5 Protection of the TSF

The MDM Server and MDM Agent work together to ensure that all security related communication between those components is protected from disclosure and modification.

Both the MDM Server and MDM Agent include self-testing capabilities to ensure that they are functioning properly. The MDM Server also has the ability to cryptographically verify during start-up that its executable image has not been corrupted.

The MDM Server also includes mechanisms (i.e., verification of the digital signature of each new image) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

4.6 TOE access

The MDM Server has the capability to display an advisory banner when users attempt to login in order to manage the TOE using the web-based and command-line based user interfaces.

4.7 Trusted path/channels

The MDM Server uses TLS/HTTPS to secure communication channels between itself and remote administrators accessing the TOE via a web-based user interface. In addition, the MDM Server implements a restricted shell (CLISH) that is accessible via SSH to provide access to low level management functions.

It also uses TLS to secure communication channels between itself and mobile device users (MD users). In this latter case, the protected communication channel is established between the MDM Server and applicable MDM Agent on the user’s mobile device.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile for Mobile Device Management, Version 2.0, 31 December 2014 (MDMPP20) with the following extended package:
- Extended Package for Mobile Device Management Agents, Version 2.0, 31 December (MDMAEP20)

That information has not been reproduced here and the MDMPP20 and MDMAEP20 should be consulted if there is interest in that material.

6 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation.

Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the Mobile Device Management Protection Profile and Extended Package for Mobile Device Management Agents and performed by the evaluation team).
- This evaluation covers only the specific software components as identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the MDMPP20, MDMAEP20, and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7 Documentation

The following documents were available with the TOE for evaluation:

- MobileIron® MobileIron Core and Android Client Mobile Device Management Protection Profile Guide, Document version 1.2, May 4, 2016

- MobileIron® On-Premise Installation Guide For MobileIron Core, Sentry, and Enterprise Connector, Core Version 9.0, Revised March 21, 2016
- MobileIron Core 9.0.0.0 Upgrade Guide, March 29, 2016.
- MobileIron® Core Device Management Guide For Android Devices, Core 9.0, Revision March 21, 2016
- MobileIron® Apps@Work Guide, MobileIron Core version 9.0, February 29, 2016
- MobileIron® Core System Manager Guide, Core version 9.0, February 26, 2016
- MobileIron® Core Command Line Interface (CLI) Reference, Core Version 9.0, February 26, 2016
- MobileIron® Core Delegated Administration, Version 9.0, February 26, 2016

Any additional customer documentation delivered with the product or available through download was not included in the scope of the evaluation and hence should not be relied upon when using the products as evaluated.

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Detailed Test Report (MDMPP20/MDMAEP20) for MobileIron Platform, version 0.3, May 27, 2016, and summarized in the Assurance Activity Report (MDMPP20/MDMAEP20) For MobileIron Platform, version 0.3, May 27, 2016 (AAR), which is publically available.

The following diagram depicts the test environments used by the evaluators.

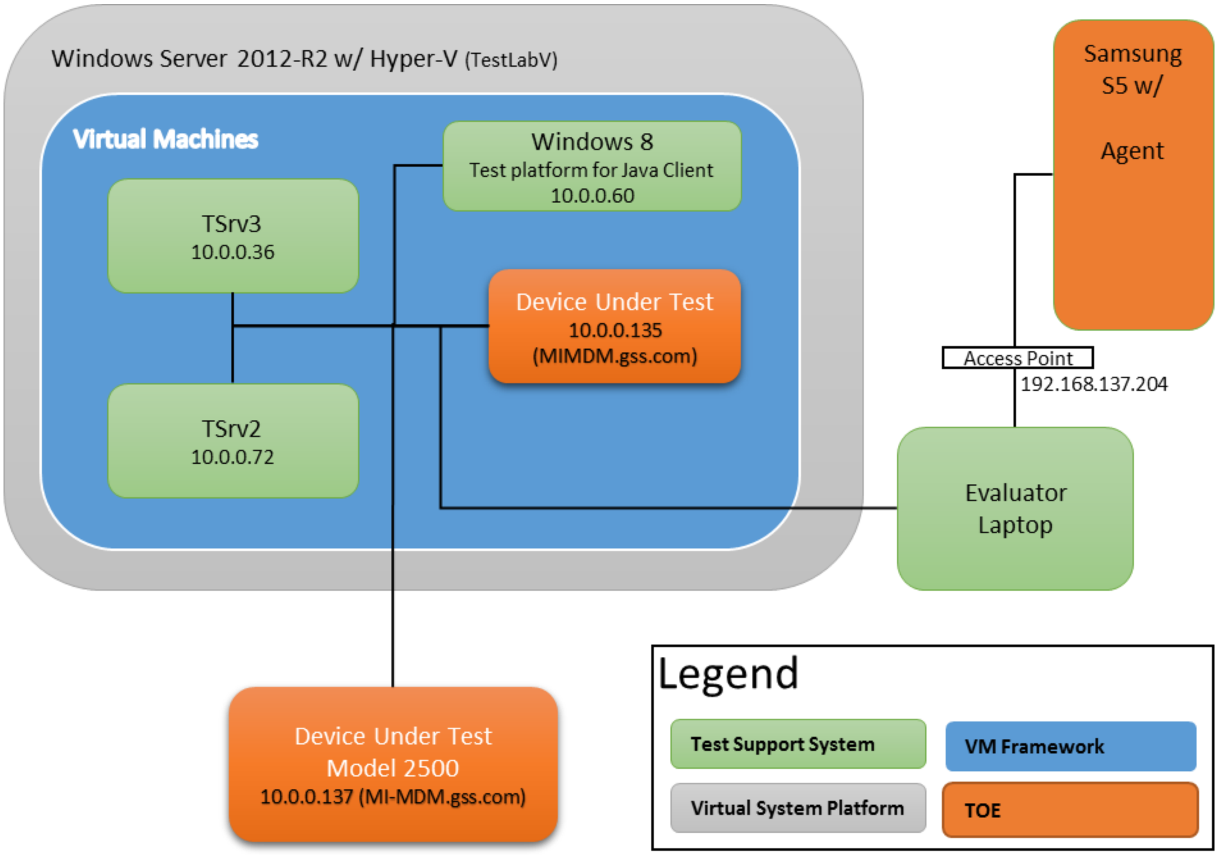

Figure 1 Test Setup

8.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the documents provided with the product as listed above, and performed the tests specified in the MDMPP20 and MDMAEP20 including the tests associated with optional requirements.

9 TOE Evaluated Configuration

The evaluated configuration consists of the following series and models:

- MobileIron Core, Version 9.0
  - Deployed on a CentOS 6.7 Linux operating system (OS) that runs on an Intel x64 architecture server platform

  - Operating on one of three physical server appliances Mobile Iron M2100, M2200, or M2500. The Mobile Iron appliances are all based on Intel Xeon CPUs (E3-1200 or E5-2670) and utilize Intel network adapters (82579LM GbE, 82574L GbE, or Quad I350 GbE) along with SATA disk drives and DRAM from 32-64 GB
  - Virtual deployments in VMWare ESXi (5.1, 5.5, or 6.0) and Microsoft Hyper-V (Server 2008 R2 or Server 2012 R2)
- MobileIron Client – Mobile@Work for Android, Version 8.6
  - NIAP requires that MDM agents be installed on NIAP-evaluated mobile devices. At present there are evaluated Samsung Galaxy mobile Android devices including Galaxy S4, Galaxy Note 3, Galaxy S5, Galaxy Note 4, and Galaxy S6 models ranging from Android version 4.4 to 5.0.2 that can be used with the Android version of the MobileIron Client.
- To use the product in the evaluated configuration, the product must be configured as specified in the accompanying *MobileIron® MobileIron Core and Android Client Mobile Device Management Protection Profile Guide*, Document version 1.2, May 4, 2016

10 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the MobileIron Platform TOE to be Part 2 extended, and to meet all applicable assurance requirements outlined by the MDMPP20 and MDMAEP20.

10.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the MobileIron Platform Version 9.0 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.2 Evaluation of the Development (ADV)

The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the MDMPP20 and MDMAEP20 related to the examination of the information contained in the TSS.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.3 Evaluation of the Guidance Documents (AGD)

The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team ran the set of tests specified by the assurance activities in the MDMPP20 and MDMAEP20 and recorded the results in an evaluation sensitive proprietary Test Report; those results are summarized in the Assurance Activities Report.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the proprietary Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities including the following terms: MobileIron, Mobile@work, Crypt-J, OpenSSH, OpenSSL, and CentOS 6. The public search for vulnerabilities and did not discover any public issues with the TOE.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: "MobileIron", "Mobile@work", "Crypt-J", "OpenSSH", "OpenSSL", and "CentOS 6".

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s testing also demonstrated the accuracy of the claims in the ST.

The validation team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

11 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR’s within the Security Target was evaluated.

All other functionality provided by the MobileIron Platform, to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. Specifically, MobileIron Sentry and additional mobile device applications, e.g., Web@work, Docs@work, AppConnect container and Secure Application Manager are not covered by the evaluation, nor are applications that may be provided with the Android mobile platforms.

Additionally, the validators advise that administrators carefully review and understand the audit process and actions required to establish and maintain audit as the TOE includes several repositories for audit data, and the export of each is accomplished separately.

12 Annexes

Not applicable.

13 Security Target

The Security Target is identified as: *MobileIron Platform (MDMPP20/MDMAEP20) Security Target, Version 1.0, May 27*, 2016.

14 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 to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **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.

15 Bibliography

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

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

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2102.

[4] Protection Profile for Mobile Device Management, Version 2.0, 31 December 2014

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

[6] MobileIron Platform (MDMPP20/MDMAEP20) Security Target, Version 1.0, May 27, 2016 (ST)

[7] Assurance Activity Report (MDMPP20/MDMAEP20) for MobileIron Platform, version 0.3, May 27, 2016 (AAR)

[8] Detailed Test Report (MDMPP20/MDMAEP20) for MobileIron Platform, version 0.3, May 27, 2016 (DTR)