National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
MobileIron Platform 11

Report Number:	**CCEVS-VR-11196-2021**
Dated:	**September 1, 2021**
Version:	**1.0**

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

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Sheldon Durrant
John Butterworth
The MITRE Corporation

Common Criteria Testing Laboratory

Cornelius Haley
John Messiha
Wasif Sikder
Raymond Smoley
Rizheng Sun
Kevin Cummins
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary 1
2 Identification 1
3 Architectural Information 3
3.1 TOE Evaluated Platforms 4
3.2 TOE Architecture 4
3.3 Physical Boundaries 5
4 Security Policy 5
4.1 Security audit 6
4.2 Cryptographic support 6
4.3 Identification and authentication 6
4.4 Security management 6
4.5 Protection of the TSF 7
4.6 TOE access 7
4.7 Trusted path/channels 7
5 Assumptions 7
6 Clarification of Scope 8
7 Documentation 8
8 IT Product Testing 9
8.1 Developer Testing 9
8.2 Evaluation Team Independent Testing 9
9 Evaluated Configuration 9
10 Results of the Evaluation 9
10.1 Evaluation of the Security Target (ASE) 10
10.2 Evaluation of the Development (ADV) 10
10.3 Evaluation of the Guidance Documents (AGD) 10
10.4 Evaluation of the Life Cycle Support Activities (ALC) 10
10.5 Evaluation of the Test Documentation and the Test Activity (ATE) 11
10.6 Vulnerability Assessment Activity (VAN) 11
10.7 Summary of Evaluation Results 11
11 Validator Comments/Recommendations 11
12 Annexes 12
13 Security Target 12
14 Glossary 12
15 Bibliography 13

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 Columbia, MD, United States of America, and was completed in September 2021. The information in this report is largely derived from the 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, and meets the assurance requirements of the Protection Profile for Mobile Device Management, Version 4.0, 25 April 2019 (MDMPP40) and the PP-Module for Mobile Device Management Agents, Version 1.0, 25 April 2019 (MDMAEP20) with the Functional Package for Transport Layer Security, Version 1.1, 1 March 2019.

The Target of Evaluation (TOE) is the MobileIron Platform 11.

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 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). 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 11 Security Target, version 0.6, August 31, 2021 and analysis performed by the Validation Team.

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) using the Common Evaluation Methodology (CEM) 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 11 (Specific models identified in Section 8)
Protection Profile	*PP-Configuration for Mobile Device Management (MDM) and MDM Agents*, Version 1.0, January 27, 2020 which includes the Protection Profile for Mobile Device Management, Version 4.0, 25 April 2019 and the PP-Module for Mobile Device Management Agents, Version 1.0, 25 April 2019 with the Functional Package for Transport Layer Security, Version 1.1, 1 March 2019
ST	MobileIron Platform 11 Security Target, version 0.6, August 31, 2021
Evaluation Technical Report	Evaluation Technical Report for MobileIron Platform 11, version 0.2, August 31, 2021
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 extended
Sponsor	MobileIron, an Ivanti Company
Developer	MobileIron, an Ivanti Company
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Sheldon Durrant, John Butterworth

3 Architectural Information

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

The Target of Evaluation (TOE) is the MobileIron Core server 11 (deployed as a VM as identified later) and associated MobileIron Client 11 agents for Android devices (Mobile@Work for Android) that are part of their MobileIron Platform. Note that the MobileIron Platform product consists of other components (MobileIron Sentry and additional mobile device applications, e.g., Mobile@Work for iOS, Web@work, Docs@work, AppConnect container and Secure Application Manager) that do not play a role in enforcing the security functions included in this Security Target.

Also, while no iOS device agent security function claims are made within this Security Target, the MobileIron Core server supports the enrollment of Apple iPad and iPhone Mobile Devices with iOS 13 (https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11036) and subsequent management of those devices via interaction with their own built in MDM agents.
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 devices (including both Android and iOS mobile devices identified in section 1.4.1.1 below), 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 later in this ST.
- Mobile content management functions are included in the MobileIron Platform, but no claims are made about those capabilities in this Security Target.

MobileIron Client– also known as Mobile@Work for Android – is an app downloaded by end users onto their mobile devices. It 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 enterprise data on the device if the user leaves or 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 this Security Target.

Note that MobileIron distributes a Mobile@Work for iOS application, however, given restrictions on the associated Apple iOS mobile devices it is incapable of implementing the required MDM agent security functions. Rather, Mobile@Work for iOS is an optional component and serves only to direct the built-in iOS MDM agent to the MobileIron Core MDM server for enrollment. As such, this component does not implement any security functions. Mobile@Work for iOS is not require to enroll an iOS device with the MobileIron Core MDM server – the Safari browser built into iOS devices can be used to enroll with the MobileIron Core MDM server with no other application support.

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the following TOE parts:

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 devices (including both Android and iOS mobile devices), application, and content management.

MobileIron Client– also known as Mobile@Work for Android – is an app downloaded by end users onto their mobile devices. It 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.

3.2 TOE Architecture

The TOE consists of two software components: MobileIron Core and MobileIron Client. MobileIron Core is a server based on a CentOS 7.6 Linux operating system (OS) with Apache 2.4 (or later) that runs on an Intel x64 architecture server platform. MobileIron supports the MobileIron Core operating as virtual deployments in VMWare ESXi (6.5, 6.7 or 7.0). MobileIron Core can optionally be configured to utilize an external LDAP server via a secure TLS channel to authenticate users.

MobileIron Client– also known as Mobile@Work for Android – is an app downloaded by end users onto their mobile devices. It 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.

Note that MobileIron distributes a Mobile@Work for iOS application, however, given restrictions on the associated Apple iOS mobile devices it is incapable of implementing the required MDM agent security functions. Rather, Mobile@Work for iOS is an optional component and serves only to direct the built-in iOS MDM agent to the MobileIron Core MDM server for enrollment. As such, this component does not implement any security functions. Mobile@Work for iOS is not required to enroll an iOS device with the MobileIron Core MDM server – the Safari browser built into iOS devices can be used to enroll with the MobileIron Core MDM server with no other application support.

NIAP requires that MDM agents must be installed on NIAP-evaluated mobile devices in order to be evaluated using the MOD-MDMA10. At present there are a number of evaluated Samsung Galaxy mobile Android devices (including Galaxy S20, Galaxy Note 10, Galaxy S21, Galaxy

XCover Pro, Galaxy S10, Galaxy A71, Galaxy Tab Active3, Galaxy Tab S4, Galaxy Note 9, Galaxy Tab S3, and Galaxy Tab Active2 models) ranging from Android version 9 to 11 that can be used with the Android version of the MobileIron Client.

MobileIron Core can manage devices with the iOS MDM agent developed and evaluated by Apple Inc. – that agent has been evaluated on Apple iPad and iPhone Mobile Devices with iOS 13.

The TOE protects itself from tampering and bypass by offering only a limited and controlled set of functions at each of its physical interfaces to its environment. Communication via those interfaces is either directed at the TOE for the purpose of administration or is directed through the TOE for communication among network devices. In both cases the TOE implements a set of policies to control the services available and those services are designed to protect and ensure the secure operation of the TOE.

3.3 Physical Boundaries

The TOE consists of two software components: MobileIron Core and MobileIron Client. MobileIron Core is a server based on a CentOS 7.6 Linux operating system (OS) with Apache 2.4 (or later) that runs on an Intel x64 architecture server platform. MobileIron supports the MobileIron Core operating as virtual deployments in VMWare ESXi (6.5, 6.7 or 7.0). MobileIron Core can optionally be configured to utilize an external LDAP server via a secure TLS channel to authenticate users.

MobileIron Client consists of apps deployed on Android mobile devices. These components are identified as the “MDM Agent”.

The TOE may be accessed and managed through a PC or terminal in the environment which must be directly connected to the TOE.

The TOE can securely export its audit records to an external IT entity in the environment for review and storage.

The TOE includes the ability to securely communicate with LDAP servers in its environment to define an enterprise-wide, user community.

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 can generate audit records for security-relevant events and includes the ability to indicate (i.e., respond) when it has been enrolled and when policies are successfully 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 with certified 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 and HTTPS 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 all the function 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 an 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.

The MDM Server can optionally be configured to use TLS to communicate with an LDAP server for user authentication.

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.

In addition, the MDM Server implements a restricted shell (CLISH) that is accessible via a console CLI to provide access to low level management functions.

5 Assumptions

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

- PP-Configuration for Mobile Device Management (MDM) and MDM Agents, Version 1.0, January 27, 2020: Protection Profile for Mobile Device Management, Version 4.0, 25 April 2019 and the PP-Module for Mobile Device Management Agents, Version 1.0, 25 April 2019 with the Functional Package for Transport Layer Security, Version 1.1, 1 March 2019

That information has not been reproduced here and the MDMPP40/MOD-MDMA10/PKGTLS11 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the MDMPP40/MOD-MDMA10/PKGTLS11 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

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 with the MDM Agents PP-Module and the TLS Functional Package and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Mobile Device Management models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- 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 MDMPP40/MOD-MDMA10/PKGTLS11 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:

- Core and Android and iOS Client Mobile Device Management Protection Profile Guide 11, Version , August 2021
- On-Premise Installation Guide for MobileIron Core and Enterprise Connector 11.0.0.0, December 3, 2020
- Getting Started with MobileIron Core 11.0.0.0, December 3, 2020
- MobileIron Core 11.0.0.0 Device Management Guide for Android and Android enterprise Devices, December 3, 2020

- MobileIron Core 11.0.0.0 Device Management Guide for iOS and macOS Devices, December 3, 2020
- MobileIron Core 11.0.0.0 System Manager Guide, December 3, 2020
- MobileIron Core 11.0.0.0 Apps@Work Guide, November 19, 2020

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured 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 proprietary Detailed Test Report for MobileIron Platform, Version 0.2, August 31, 2021 (DTR), as summarized in the evaluation Assurance Activity Report.

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 a Common Criteria Certification document and ran the tests specified in the MDMPP40/MOD-MDMA10/PKGTLS11 including the tests associated with optional requirements. The AAR, in sections 1.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

9 Evaluated Configuration

See Section 3.1.

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 assurance activities and 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 5 and CEM version 3.1 rev 5. The evaluation determined the MobileIron Platform TOE to be Part 2 extended, and to meet the SARs contained in the MDMPP40/MOD-MDMA10/PKGTLS11.

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 11 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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 applied each ADV CEM work unit. 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 MDMPP40/MOD-MDMA10/PKGTLS11 related to the examination of the information contained in the TSS.

The validator 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 applied each AGD CEM work unit. 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 validator 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 applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator 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 applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the MDMPP40/MOD-MDMA10/PKGTLS11 and recorded the results in a Test Report, summarized in the AAR.

The validator 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 Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

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: “Ivanti”, “Mobile Iron”, Mobile@work”, “Openssl”, “Bouncy Castle”, “GNU Core Utilities”, “CentOS 7.6”, Apache 2.4” and “Xeon E5”.

The validator 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.

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 11 Security Target, Version 0. 0.6, August 31, 2021*.

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 5, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, September 2102.

[4] Protection Profile for Mobile Device Management, Version 4.0, 25 April 2019 (MDMPP40) and the PP-Module for Mobile Device Management Agents, Version 1.0, 25 April 2019 (MDMAEP20) with the Functional Package for Transport Layer Security, Version 1.1, 1 March 2019.

[5] MobileIron Platform 11 Security Target, Version 0.6, August 31, 2021 (ST).

[6] Assurance Activity Report for MobileIron Platform 11, Version 0.2, August 31, 2021 (AAR).

[7] Detailed Test Report for MobileIron Platform 11, Version 0.2, August 31, 2021 (DTR).

[8] Evaluation Technical Report for MobileIron Platform, Version 0.2, August 31, 2021 (ETR)