National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report

for

Microsoft Intune

Report Number: CCEVS-VR-VID11298-2024

Dated: 31 December 2024

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

Swapna Katikaneni

Dr. Jerome Myers

The Aerospace Corporation

Dr. Jade Stewart

Department of Defense

Common Criteria Testing Laboratory

Joon Sim

Kevin Steiner

Lightship Security, USA

Table of Contents

List of Tables

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Microsoft Intune (2411) and Microsoft Company Portal App (for Android), v5.0.6375.0 (7015796) provided by Microsoft Corporation. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in December 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). 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 and PP-Module for MDM Agents, Version 1.0.

The TOE is Microsoft Intune (2411) and Microsoft Company Portal App (for Android), v5.0.6375.0 (7015796). The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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 VR applies only to the specific versions of the TOE as evaluated. 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 ETR 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 ETR are consistent with the evidence produced.

Intune is a FedRAMP authorized Cloud service in Azure, part of the Deployment Model Government Community Cloud (Package ID F1603087869) and the Public Cloud (Package ID F1209051525).

Microsoft Azure Government has continued Provisional Authorization to Operate (P-ATO) based on the FedRAMP Joint Authorization Board (JAB) review of Microsoft Azure's Government 2024 annual assessment package (letter from FedRAMP Directory dated 11/26/24). Intune is listed as a service in the FedRAMP High Baseline System Security Plan (SSP) for Microsoft Azure Government version 1.0 dated 9/16/24 which was submitted as part of Microsoft's 2024 annual assessment.

Microsoft lists the Intune service as FedRAMP High (P-ATO issued by the JAB) and DoD IL2 (PA issued by DISA). https://learn.microsoft.com/en-us/azure/azure-government/compliance/azure-services-in-fedramp-auditscope

The technical information included in this report was obtained from the *Microsoft Intune Security Target*, Version 1.4, December 2024 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 TOE: the fully qualified identifier of the product as evaluated.
- The 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
Evaluated Product	Microsoft Intune (2411) Microsoft Company Portal App (for Android), v5.0.6375.0 (7015796)
Sponsor and Developer	Microsoft Corporation
CCTL	Lightship Security USA 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
CEM	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017.

Item	Identifier
Protection Profile	Protection Profile for Mobile Device Management, Version 4.0, 2019-04-25 PP-Module for MDM Agents, version 1.0, 2019-04-25
ST	Microsoft Intune Security Target, Version 1.4, December 2024
Evaluation Technical Report	Microsoft Intune Evaluation Technical Report, Version 1.4, December 2024
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Evaluation Personnel	Lightship USA: Joon Sim, Kevin Steiner
CCEVS Validators	Aerospace Corporation: Swapna Katikaneni, Dr. Jerome Myers Department of Defense: Dr. Jade Stewart

3. Architectural Information

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

Microsoft Intune is a mobile device management system that includes MDM Server and Mobile Application Store (MAS) functionality. The Microsoft Company Portal app provides the MDM agent for Android devices.

3.1. TOE Evaluated Configuration

Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). Administrators can control how their organization's mobile devices are used and also configure specific policies to control applications installed on the devices. There is only one Intune service (version) that is continuously offered with rolling feature enhancements which is located at the URL described in section 1.2 of the Security Target. Intune is part of Microsoft's Enterprise Mobility + Security (EMS) suite.

The Microsoft Intune Company Portal is a mobile device management agent.

3.2. Physical Boundary

Microsoft Intune is the service available at https://intune.microsoft.com

Microsoft Intune is built on Azure Virtual Machines with the following underlying platform components:

a) **Operating System.** Microsoft Windows Server comprising of the following versions:

   i. **Microsoft Windows Server 2019 Datacenter**

Microsoft Intune Company Portal is the application installed on mobile devices to facilitate enrollment and command execution. The TOE was tested on the following mobile device platforms:

a) Android 13 with Microsoft Intune Company Portal version 5.0.6375.0 (7015796)

b) Android 11 with Microsoft Intune Company Portal version 5.0.6375.0 (7015796)

The administrator and user must follow the instructions in the Microsoft Intune Operational and Administrative Guidance, v1.2 to configure and remain in the evaluated configuration.

3.3. Required Non-TOE Hardware, Software, and Firmware

The TOE operates with the following components in the environment:

a) Mobile Devices. The TOE supports Android and iOS based mobile devices and was tested with:
   i. iOS 15 executing on the following hardware:
      - iPhone 12
   ii. Android 13 executing on the following hardware:
      - Samsung Galaxy S21 Ultra 5G
   iii. Android 11 executing on the following hardware:
      - Google Pixel 4a 5G

   Note: The Intune service also supports the management of devices listed at https://learn.microsoft.com/en-us/mem/intune/fundamentals/supported-devices-browsers however these devices were not tested as part of this evaluation.

b) Audit Server. The TOE can send audit events to any endpoint that is able to use Microsoft Graph API via HTTPS.

4. Security Policy

This section summarizes the security functionality of the TOE:

4.1. Security Audit

Microsoft Intune has the ability to generate, review, protect, and restrict access to audit and event logs as required by the MDM PP and MDM Agent PP-Module. Audit information generated by the system includes the date and time of the event, the user identity that caused the event to be generated, and other event specific data. Authorized administrators can review audit logs and have the ability to search and sort audit records securely via the Microsoft Intune Admin Center console or via the Graph API. In the context of this evaluation, the protection profile requirements cover generating audit events, which events should be audited, and providing secure storage for audit event entries.

4.2. Cryptographic Support

Microsoft Intune provides cryptographic functions that support encryption/decryption, cryptographic signatures, cryptographic hashing, cryptographic key agreement, and random number generation. The TOE additionally provides support for X.509 certificates including validation functions. Certificates are issued during device enrollment and are used for authentication and protection of both user and system data while in transit.

4.3. Identification and authentication

Each Microsoft Intune administrator must be identified and authenticated based on administrator-defined policy prior to performing any TSF-mediated functions. An interactive user invokes a trusted path to protect their identity and credentials. Microsoft Intune maintains databases of accounts including their identities, authentication information, group associations, and administrative privileges. Microsoft Intune provides the ability to use, store, and protect X.509 certificates that are used for mobile devices. Communications between the Mobile device and Intune are facilitated with authenticated TLS sessions.

4.4. Security Management

Microsoft Intune includes several functions to manage security policies on registered devices. Microsoft Intune MDM policy functions include the ability to define the minimum password length, the number of failed logon attempts, the duration of lockout, and password age. MDM Policy management is available to Intune administrators that have sufficient permissions or are members of an applicable role-based group as described in FMT_SMR.1. Successfully enrolled devices are issued an X.509 certificate that is used for identification and authentication.

4.5. Protection of the TOE Security Functions

Microsoft Intune provides several features to ensure the protection of TOE security functions. Intune protects against unauthorized data disclosure and modification by requiring authenticated TLS sessions between registered devices and Intune. All Intune components employ self-testing features on start-up that ensure the integrity of executable code and any cryptographic functions.

4.6. Trusted path/Channels for Communications

Microsoft Intune uses TLS and HTTPS to provide a trusted path for communications between Intune and remote administrators as well as registered devices. Trusted channels provided by Intune include the Microsoft Intune Admin Center for Administrator use via HTTPS, and a X.509 authenticated TLS channel for device enrollment and continual policy updates.

5. Assumptions

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

- *Protection Profile for Mobile Device Management, Version 4.0, 2019-04-25*
- *PP-Module for MDM Agents, version 1.0, 2019-04-25*

That information has not been reproduced here and PP_MDM_V4.0 and MOD_MDM_AGENT_V1.0 should be consulted if there is interest in that material.

6. Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in PP_MDM_V4.0 and MOD_MDM_AGENT_V1.0 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.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. 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 in accordance with the assurance activities specified in the PP_MDM_V4.0 and MOD_MDM_AGENT_V1.0 Supporting Document and performed by the Evaluation team
- This evaluation covers only the specific software version 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 PP_MDM_V4.0 and MOD_MDM_AGENT_V1.0 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.
- The Intune TOE supports Apple iOS devices via the native iOS MDM agent. The iOS agents are evaluated as part of the Apple iOS evaluations and not part of this evaluation. Intune was tested to ensure it can manage those devices, but the agent’s behavior on those devices was not otherwise tested.

7. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *Microsoft Intune Operational and Administrative Guidance,* Version 1.2, December 2024

The above document makes reference to additional Microsoft documentation that may be useful for understanding the administration and use of the TOE. However, the above document is considered to be self-contained for the purpose of the evaluation. Those supplemental references were not covered by the scope of the evaluation and are not considered to be trusted for the configuration, administration, and use of the TOE.

8. IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in *Microsoft Intune MDM 4.0 Detailed Test Report*, which is not publicly available. The *Microsoft Intune Assurance Activity Report*, Version 1.4, December 2024 provides an overview of testing and the prescribed assurance activities.

8.1. Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2. Evaluation Team Independent Testing

Testing of the TOE was performed by Lightship Security USA from February 2023 through December 10, 2024, at the Lightship Security USA CCTL facility.

Not all test cases were able to be run independently by the evaluation lab. To satisfy these tests, onsite/remote vendor engagement was needed. Onsite testing was performed at Microsoft Studio A, 15291 NE 40th St, Redmond, WA 98052. Remote testing was performed over a Lightship hosted Microsoft Teams session, except when evidence was exchanged via email. NIAP approved and participated in the onsite/remote test activities. The vendor, validation team and evaluation lab also participated in the onsite and remote sessions.

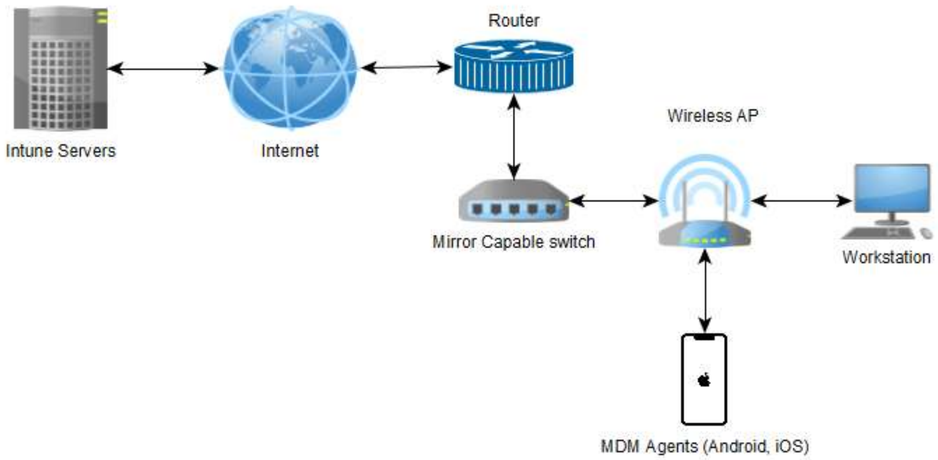
The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Assurance Activities.

Each Assurance Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

8.3. Evaluated Configuration

The TOE testing environment is depicted in the following diagram:



The devices in the testing environment included the following configuration/software:

Workstation #1

- Windows 10 Pro 22H2 (OS build 19045.5198)
- Wireshark (Version 3.6.16)
- Brave browser (Version 1.73.91)
- Google Chrome (Version 131.0.6778.86)

Workstation #2

- Windows 11 23H2 (OS build 22631.4541)
- Wireshark (Version 3.6.16)
- Google Chrome (Version 131.0.6778.86)

iPhone-1 (iOS Agent #1)

- iOS 15.2.1
- Company Portal application (Version 5.2409.0)

iPhone-2 (iOS Agent #2)

- iOS 15.1.1
- Company Portal application (Version 5.2409.0)

iPhone-3 (iOS Agent #3)

- iOS 15.2.1
- Company Portal application (Version 5.2409.0)

Google Pixel 4a 5G (Android)

- Android 11
- Company Portal application (Version 5.0.6375.0)

Samsung Galaxy S21 Ultra S21 Ultra 5G (Android)

- Android 13
- Company Portal application (Version 5.0.6375.0)

9. Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that all 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 Revision 5 and CEM Version 3.1 Revision 5. The evaluation determined the Microsoft Intune (2411) and Microsoft Company Portal App (for Android), v5.0.6375.0 (7015796) to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in PP_MDM_V4.0 and MOD_MDM_AGENT_V1.0 Supporting Document.

9.1. Evaluation of 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 Microsoft Intune (2411) and Microsoft Company Portal App (for Android), v5.0.6375.0 (7015796) that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team 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.

9.2. Evaluation of Development Documentation (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 ST and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the PP_MDM_V4.0 and MOD_MDM_AGENT_V1.0 Supporting Document related to the examination of the information contained in the TSS.

The Validation 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.

9.3. Evaluation of 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 Validation team 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.

9.4. Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

The Validation team 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.

9.5. Evaluation of 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 PP_MDM_V4.0 and MOD_MDM_AGENT_V1.0 Supporting Document and recorded the results in a Test Report, summarized in the AAR.

The Validation team 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.

9.6. Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the *Microsoft Intune MDM 4.0 Vulnerability Assessment*, Version 1.3, December 2024, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on December 17, 2024, did not uncover any residual vulnerability.

The Evaluation team searched:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
    - Common Vulnerabilities and Exposures: https://cve.mitre.org/cve/ https://www.cvedetails.com/vulnerability-search.php
    - US-CERT: http://www.kb.cert.org/vuls/html/search

- Cloud Vulnerabilities and Security Issues Database: https://www.cloudvulndb.org/

The Evaluation team performed a search using the following keywords:

- Microsoft Intune
- Intune
- Azure Active Directory
- Microsoft Endpoint Manager (Note: this is a legacy term)
- Microsoft Endpoint Manager Admin Center (Note: this is a legacy term)
- Microsoft Intune Admin Center
- Mobile Device Management
- Microsoft Graph API
- Azure Tenant
- Microsoft Company Portal
- Mobile Application Management
- Microsoft Enterprise Mobility + Security (EMS) suite
- Schannel
- Mobile Application Store

The Validation team 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.

The evaluation team reviewed the vendor’s processes to ensure that the vulnerabilities are appropriately mitigated. As per the vendors assertion, Microsoft Intune in their Government Cloud environment has no High-Risk vulnerabilities (adjudicated by the FedRAMP program's guidelines) as of the date of submission to NIAP.

9.7. 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 test activities 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 performed the Assurance Activities in the PP_MDM_V4.0 and MOD_MDM_AGENT_V1.0 Supporting Document and correctly verified that the product meets the claims in the ST.

10. Validator Comments

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documentation referenced in Section 7 of this Validation Report. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the TOE is configured as evaluated. 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 be relied upon when configuring or operating the TOE as evaluated.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

This evaluation is the first NIAP evaluation completed for a cloud service-based product against the Mobile Device Management Protection Profile Version 4.0. Although the PP had been developed with cloud-services in mind, it was expected that, as with the first evaluation of any technology type against a PP, the evaluation would identify security requirements and evaluation activities that needed clarification. There were numerous NIAP Technical Queries that resulted from this evaluation and associated validation. Some queries resulted in Technical Decisions that are identified in the Security Target and elaborated upon in the Assurance Activity Report. Other queries require more discussion before a Technical Decision can be issued. In addition, there were other recommendations for improvements in the next iteration of the PP that were identified, but were not considered appropriate for Technical Decisions against the current PP. For example, the MDM PP 4.0 allows for communication selections that could result in vulnerabilities.

It is recommended that penetration testing be performed for possible attack vectors that could uncover vulnerabilities/Cloud vulnerabilities that are not addressed through the current MDM PP's Security Functional Requirements. For this validation, NIAP relied on FedRAMP for this aspect of cloud certification as well as DoD Service Component Red Team testing.

The Microsoft’s FedRAMP documentation was reviewed. This, plus some extra documentation that Microsoft provided upon request for review, helped satisfy MDM PP 4.0's Trusted Update requirements. For the evaluation activity of AGD_OPE.1.1E, it is suggested that the PP be adapted through a TD to more directly address update models for cloud products.

Potential users should be aware that the updates to the Intune server portion of the TOE are not under the control of the tenant administrator but are controlled by the Azure platform administrator.

The evaluation spanned several releases of the TOE due to the update model associated with this implementation and the results are considered applicable to the version identified in this VR due to the regression testing performed on each release by the vendor.

11. Annexes

Not applicable.

12. Security Target

Microsoft Intune Security Target, Version 1.4, December 2024.

13. GLOSSARY

- **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.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **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.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

15. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001*, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2017-04-002,* Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2017-04-003,* Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004*, Version 3.1, Revision 5, April 2017
5. *Protection Profile for Mobile Device Management, Version 4.0, 2019-04-25*
6. *PP-Module for MDM Agents, Version 1.0, 2019-04-25*
7. *Supporting Document, Mandatory Technical Document, PP-Module for MDM Agents, Version 1.0, 2019-04-25*
8. *Microsoft Intune Security Target*, Version 1.4, December 2024
9. *Operational and Administrative Guidance Microsoft Intune*, Version 1.2, December 2024
10. *Microsoft Intune Assurance Activity Report*, Version 1.4, December 2024
11. *Microsoft Intune MDM 4.0 Vulnerability Assessment*, Version 1.3, December 2024
12. *Microsoft Intune Evaluation Technical Report,* Version 1.4, December 2024
13. *Microsoft Intune MDM 4.0 Detailed Test Report*, Version 1.4, December 2024
14. *Microsoft Intune MDM v4.0 Test Evidence,* Version 1.3, December 2024