National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report for

IBM MaaS360 Cloud Extender version 3.000.800

Report Number:	CCEVS-VR-VID11531-2025
Dated:	September 02, 2025
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

Jerome Myers, Ph.D.

Patrick Mallett, Ph.D.

The Aerospace Corporation

Anne Gugel

Farid Ahmed, Ph.D.

Johns Hopkins University Applied Physics Lab

Common Criteria Testing Laboratory

Joachim Vandersmissen

Amr Said

Parker Collier

Walker Riley

atsec information security corporation

Austin, TX

Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of IBM MaaS360 Cloud Extender version 3.000.800 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

This VR is intended to assist the end-user of this product and any security certification agent for that end- user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target ([ST]), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the validator comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by atsec Common Criteria Testing Laboratory (CCTL) in Austin, TX, USA, and was completed in September 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by atsec. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Extended and meets the assurance requirements of the *Protection Profiles* and *Functional Packages* identified in Table 1.

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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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 IT 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 Product Compliant List (PCL).

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

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The *PPs/PP-Modules/Packages* 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	IBM MaaS360 Cloud Extender version 3.000.800
Security Target	IBM MaaS360 Cloud Extender version 3.000.800 Security Target Version 1.3, 2025-08-12

Sponsor & Developer	International Business Machines (IBM) Corporation
Completion Date	September 2025
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	Protection Profile for Application Software, Version 1.4, 2021-10-07 ([PP_APP_v1.4]] Functional Package for TLS, Version 1.1, 2019-03-01 ([PKG_TLS_V1.1])
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 extended
CCTL	atsec information security corporation 4516 Seton Center Parkway Suite 250 Austin, TX 78759
Validation Personnel	Jerome Myers, Patrick Mallett, Anne Gugel, Farid Ahmed
Evaluation Personnel	Joachim Vandersmissen, Amr Said, Parker Collier, Walker Riley

3 TOE Architecture

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

The TOE is the IBM Cloud Extender (CE) application. It consists of four modules enabling communications functionality with various customer-provided services and the IBM MaaS Cloud Extender Configuration Tool, hereafter refers to as Configuration Tool.

The TOE is installed within the customer's network in order to enable services offered by the IBM MaaS360 Enterprise Mobility Management (EMM), a cloud-based multi-tenant platform that provides a mobile device management (MDM) solution. Specifically, the TOE is installed behind the customer firewall with network access to appropriate internal systems. The TOE is available as a small Windows Application.

The four TOE modules covered by the evaluation are the following:

- Exchange Integration Module: this module interacts with the Exchange Server to automatically discover ActiveSync-connected devices, and uploads that device information to the IBM MaaS360 Cloud.
- User Authentication Module: this module interacts with Active Directory or LDAP directories to provide user authentication service for various MaaS360 functions, such as self-service device enrollment with corporate credentials, MaaS360 Portal login, and user management portal.
- User Visibility Module: this module uses the corporate directory groups to allow for the assignment and distribution of policies, apps, and content to mobile devices.
- Certificate Integration Module: this module facilitates the automatic provisioning, distribution, and renewal of digital identity certificates to managed mobile devices by using existing Microsoft Certificate Authority (CA), Symantec® CA, or Entrust® Admin Services and Identity Guard.

4 Environmental Strengths

The TOE provides the following security functions as described in the ST.

4.1 Cryptographic Support

The TOE provides the following cryptographic functions via the Microsoft Cryptography API: Next Generation (CNG) cryptographic library from the underlying Microsoft Windows Server platform on which the TOE runs:

- TLS v1.2 connections: the TOE communicates with the Exchange Server, Domain Controller, and PKI Certificate Servers.
- Protecting data-at-rest using the Encrypted File System (EFS) for directory that contains all configuration and log information.
- Encrypting registry entries using Data Protection Application Programming Interface (DPAPI).

The TOE also comes with its own OpenSSL cryptographic library, which provides the following cryptographic services:

- TLS v1.2 connections to the MaaS360 Portal and Simple Certificate Enrollment Protocol (SCEP) certificate servers.
- Device and user certificate generation for certificate signing requests to a SCEP server.

4.2 User Data Protection

The TOE provides user data protection services by restricting its access to specific platform-based resources, such as sensitive data repositories, and network communications, that are strictly needed to support the necessary TOE functionality.

Sensitive application data when stored in non-volatile memory is protected using platform-provided EFS services.

4.3 Identification and Authentication

The TOE supports authentication by X.509 certificates by the TOE and by using the platform API.

4.4 Security Management

The TOE provides the ability to set a number of its configuration options, which are stored, as recommended by Microsoft, in the Windows Registry and are protected using the Data Protection Application Programming Interface (DPAPI).

4.5 Privacy

The TOE does not specifically request Personally Identifiable Information (PII).

4.6 Protection of the TSF

The TOE only uses documented Windows APIs. The TOE does not write user-modifiable files to directories that contain executable files. The TOE implements anti-exploitation capabilities including stack buffer overrun protection and Address Space Layout Randomization (ASLR) techniques.

The TOE is packaged and delivered in the Windows Application Software (.EXE) format signed with Microsoft Authenticode using the Microsoft Sign Tool.

4.7 Trusted Path/Channel

The TOE protects all transmitted data via trusted channels over TLS 1.2.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the *PPs, PP-Modules,* and *Packages* to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed *PPs, PP-Modules,* and *Packages*, as listed in Table 1.

5.2 Clarification of Scope

As with any evaluation, this evaluation shows only that the evaluated configuration meets the security claims made, with a certain level of assurance, achieved through performance by the evaluation team of the evaluation activities specified by the *PPs*, *PP-Modules*, and *Packages* specified in Table 1.

- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in IBM MaaS360 Cloud Extender version 3.000.800, August 12, 2025 ([ST]). Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- 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 TOE must be installed, configured, and managed as described in the documentation referenced in Section 6 of this VR.

6 Documentation

The vendor provides guidance documents describing the installation process for IBM MaaS360 Cloud Extender version 3.000.800, as well as guidance for subsequent administration and use of the applicable security features.

The following guidance documentation was examined during the evaluation:

- MaaS360 Cloud Extender Common Criteria Guide, Version 1.1 ([CCGUIDE])

To use the TOE in the evaluated configuration, the product must be configured as specified in the guidance documentation listed above. Consumers are encouraged to download this documentation from the NIAP website. Only the guidance documentation listed above, and the specified sections of the other documents referenced by that guide should be trusted for the installation, administration, and use of the TOE in its evaluated configuration. Any other documentation (e.g., published on the vendor's website) was not covered by the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated.

7 IT Product Testing

A non-proprietary description of the tests performed, and their results is provided in Section 2 of the Assurance Activity Report ([AAR]).

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the *PPs*, *PP-Modules*, and *Packages* listed in Table 1.

7.1 Developer Testing

No evidence of developer testing is required by the assurance activities for this TOE.

7.2 Evaluation Team Testing

The evaluation team established a test configuration comprising IBM MaaS360 Cloud Extender version 3.000.800 running on platform Dell PowerEdge R740. Section 2.3.4 of the Assurance Activity Report ([AAR]) provides a detailed description of the test configuration the CCTL used to test the TOE, including a description of the test environment and a list of tools used.

The evaluation team devised a Test Plan based on the Test Activities specified in the above *PP* and *Functional Package*. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at the atsec CCTL facility in Austin, TX, from May 2025 to August 2025.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements were fulfilled.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The evaluated configuration consists of the following hardware and software when configured in accordance with the documentation specified in section 6:

- Operating system: Microsoft Windows Server 2019 Standard version 1809 (x64)
- Hardware: Dell PowerEdge R740 with an Intel Xeon Gold 5120 processor (SkyLake microarchitecture)

8.2 Excluded Functionality

The following modules are part of the MaaS360 Cloud Extender product but are not delivered with the TOE and therefore the services they provide are excluded from the evaluated configuration.

- Email Notification module
- IBM Traveler Integration module
- Mobile Enterprise Gateway (MEG) module

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for IBM MaaS360 Cloud Extender version 3.000.800 ([*ETR*]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

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 ([CCPART1], [CCPART2], [CCPART3]) and CEM version 3.1, revision 5 ([CEM]), and the specific evaluation activities specified in the *PPs*, *PP-Modules*, and *Packages* listed in Table 1.

The evaluation determined the TOE satisfies the conformance claims made in the IBM MaaS360 Cloud Extender version 3.000.800 Security Target, of Part 2 extended and Part 3 extended. The TOE satisfies the requirements specified in the *PPs*, *PP-Modules*, and *Packages* listed in Table 1.

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

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS assurance activity and each CEM work unit from ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_SPD.1, and ASE_TSS.1. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed *PPs*, *PP-Modules*, and *Packages*, and security function descriptions that satisfy the requirements.

9.2 Evaluation of the Development Activities (ADV)

The evaluation team performed each ADV assurance activity and applied each CEM work unit from ADV_FSP.1. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed *PPs, PP-Modules*, and *Packages* for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

9.3 Evaluation of the Guidance Activities (AGD)

The evaluation team performed each AGD assurance activity and applied each CEM work unit from AGD_OPE.1 and AGE_PRE.1. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC assurance activity and applied each CEM work unit from ALC_CMC.1 and ALC_CMS.1 to the extent possible given the evaluation evidence required by the claimed *PPs*, *PP-Modules*, and *Packages.* The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

9.5 Evaluation of the Test Documentation and the Test Activities (ATE)

The evaluation team performed each ATE assurance activity and applied each CEM work unit from ATE_IND.1. The evaluation team ran the set of tests specified by the claimed *PPs*, *PP-Modules*, and *Packages* and recorded the results in the Test Report, summarized in the AAR.

9.6 Evaluation of the Vulnerability Assessment Activity (AVA)

As required by NIAP Policy 17 Addendum – vulnerability mitigation guidance, the following search terms were used during the vulnerability search:

Cloud Extender	bitlib	Gloox
MaaS360	Boost	Protocol buffers
log4net	Paho	libcurl

libest	Microsoft Concurrency Runtime Library	SharpZipLib
Lua	Microsoft C Runtime Library	SQLite
Lua cURL	Microsoft Visual C++ Redistributable	zlib
LuaSql	OpenSSL	InstallShield
lua-winreg		Cryptography Next Generation

The evaluator searched for publicly known vulnerabilities using the following sources:

MITRE Common Vulnerabilities and Exposures (CVE) List:

https://cve.mitre.org/cve/

National Vulnerability Database:

https://nvd.nist.gov/

CISA Known Exploited Vulnerabilities Catalog:

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

OpenSSL Vulnerabilities

https://openssl-library.org/news/vulnerabilities-1.0.2/

SQLite Vulnerabilities

https://sqlite.org/cves.html

libcurl vulnerabilities

https://curl.se/docs/security.html

The vulnerability search was repeated throughout the evaluation process. The last vulnerability search was performed on 2025-08-19.

All “crucial” vulnerabilities (as defined by the NIAP Policy 17 Addendum) found during the vulnerability search were mitigated. Any residual vulnerabilities are not considered crucial.

Subsequently, the evaluator performed a generic port scan on the TOE to search for any undocumented open network ports. The evaluator found that no ports are unexpectedly open. In other words: all ports are either expected to be open as part of the operational environment or are associated with the TOE and publicly documented as such.

Finally, as required by the assurance activity, the evaluator ran a virus scan against the TOE directory C:\Program Files (x86). The evaluation team performed each AVA assurance activity and applied each CEM work unit from AVA_VAN.1. The evaluation team performed a vulnerability analysis following the processes described in the claimed *PPs*, *PP-Modules*, and *Packages*. This comprised a search of public vulnerability databases on August 19, 2025.

In addition to the lists of fixes published by the vendor, the evaluator performed manual searches throughout the evaluation process. The most recent searches did not identify any crucial vulnerabilities that were not addressed prior to product placement on the NIAP PCL. The conclusion drawn from the vulnerability analysis is that no crucial residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the evaluation activities specified in the claimed *PP*. Furthermore, the evaluation team’s testing demonstrates 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.

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the guidance documents listed in Section 6. No other versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target and in sec 5 of this document. Other functionality included in the product was not assessed as part of this evaluation. Specifically, note the Excluded Functionality, described in Section 8.2. All other concerns and issues are adequately addressed in other parts of this document.

The vendor provided a Software Bill of Materials (SBOM), as NIAP policy requires. NIAP has reviewed it, but the SBOM process is still being piloted. This SBOM was not used by the validators for any specific validation activities.

11 Security Target

The ST for this product's evaluation is IBM MaaS360 Cloud Extender version 3.000.800 Security Target, Version 1.3, dated 2025-08-12 ([ST]).

A Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
PCL	Product Compliant List
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VR	Validation Report

B Bibliography

The validation team used the following documents to produce this VR:

[CCPART1]	Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.
[CCPART2]	Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
[CCPART3]	Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017.
[CEM]	Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.
[PP_APP_v1.4]	Protection Profile for Application Software, Version 1.4, 2019-03-01
[PKG_TLS_V1.1]	Functional Package for TLS Version 1.1, 2019-03-01
[ST]	IBM MaaS360 Cloud Extender version 3.000.800 Security Target, Version 1.3, 2025-08-12
[CCGUIDE]	MaaS360 Cloud Extender Common Criteria Guide, Version 1.1, 2025-08-12
[ETR]	Evaluation Technical Report IBM MaaS360 Cloud Extender version 3.000.800, Version 1.1, 2025-08-19
[AAR]	Assurance Activity Report IBM MaaS360 Cloud Extender version 3.000.800, Version 1.2, 2025-08-29