# National Information Assurance Partnership
# Common Criteria Evaluation and Validation Scheme


# Validation Report

# IBM MaaS360 2.106.500.016 Cloud Extender

**Report Number: CCEVS-VR-VID11113-2022**

**Dated: September 12, 2022**

**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 George G. Meade, MD 20755-6982**

# ACKNOWLEDGEMENTS


## Validation Team

Patrick W Mallett, Ph.D.
Jerome F. Myers, Ph.D.
*The Aerospace Corporation*

Farid Ahmed
Anne T. Gugel
*John Hopkins University Applied Physics Laboratory*

## Common Criteria Testing Laboratory

King Ables
Elliot Keen
Randy Baker
Scott Chapman
*atsec information security corporation, Austin, TX*

# Table of Contents

# 1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of IBM MaaS360 2.106.500.016 Cloud Extender provided by IBM Corp. It presents the evaluation results, their justifications, and the conformance results. This Validation Report 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 Common Criteria Testing Laboratory (CCTL) atsec information security corporation in Austin, TX, United States of America, and was completed in September 12, 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CCTL, atsec information security corporation. The evaluation determined that the product is both Common Criteria (CC) Part 2 Extended and Part 3 Conformant, and meets the assurance requirements given in:

- Protection Profile for Application Software, Version 1.3, 2019-03-01 (pp_app_v1.3), [ASPPv1.3]
- Functional Package for TLS, Version 1.1, 2019-03-01 (pkg_tls_v1.1), [TLSPKGv1.1]

The TOE is IBM MaaS360 2.106.500.016 Cloud Extender executing on the following operating system and hardware platform:

- Operating system: Microsoft Windows Server 2019 Standard version 1809 (x64)
- Hardware: Dell PowerEdge R740 with an Intel Xeon Gold 5118 processor (SkyLake microarchitecture).

The TOE identified in this Validation Report has been evaluated at a NIAP approved CCTL using the "Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5)" (CEM) for conformance to the "Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5)" (CC) and the Assurance Activities (AA) of the aforementioned Protection Profile. 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 (CCEVS) 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, reviewed testing activities, 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 the functional requirements and assurance requirements stated in the Security Target (ST). 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 CCTL atsec information security corporation evaluation team concluded that the CC requirements specified by:

- Protection Profile for Application Software, Version 1.3, 2019-03-01
- Functional Package for TLS, Version 1.1, 2019-03-01

have been met.

The technical information included in this report was obtained from IBM MaaS360 2.106.500.016 Cloud Extender Security Target (ST) Version 1.4 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) for Evaluation Assurance 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 Product Compliant List.

The following table provides information needed to completely identify the product, including the following.

- 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 results of the evaluation
- The Protection Profile (PP) to which the product is conformant
- The organizations and individuals participating in the evaluation

| Item | Identifier |
|---|---|
| **Evaluation Scheme** | United States NIAP Common Criteria Evaluation and Validation Scheme |
| **TOE** | The TOE IBM MaaS360 2.106.500.016 Cloud Extender executing on the following operating system and hardware platforms:<br>• Operating system: Microsoft Windows Server 2019 Standard version 1809 (x64)<br>• Hardware: Dell PowerEdge R740 with an Intel Xeon Gold 5118 processor (SkyLake microarchitecture). |
| **PP** | • Protection Profile for Application Software, Version 1.3, 2019-03-01 |

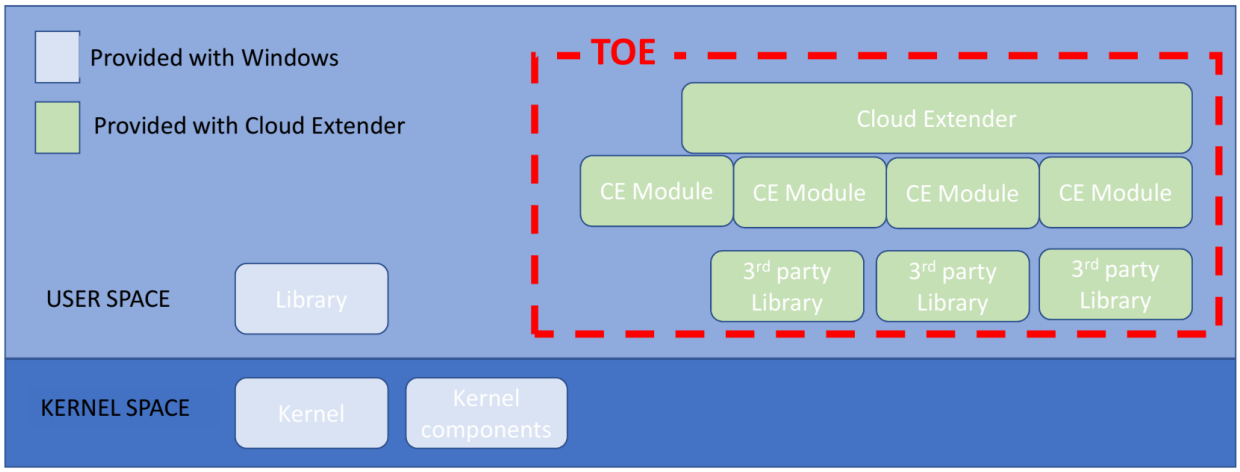
| Item | Identifier |
|---|---|
| | • Functional Package for TLS, Version 1.1, 2019-03-01 |
| **ST** | IBM MaaS360 2.106.500.016 Cloud Extender Security Target, Version 1.4, dated 2022-07-20 |
| **ETR** | Evaluation Technical Report for a Target of Evaluation IBM MaaS360 2.106.500.016 Cloud Extender Version 1.0, dated 2022-08-15 |
| **CC Version** | Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 |
| **Conformance Result** | CC Part 2 extended, CC Part 3 extended |
| **Sponsor** | IBM Corp. |
| **Developer** | IBM Corp. |
| **CCTL** | atsec information security corporation, Austin, TX |
| **CCEVS Validators** | Patrick W Mallet, Jerome F. Myers, Farid Ahmed, Anne T. Gugel |

# 3. Architectural Information

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

The Target of Evaluation (TOE) is a Microsoft Windows application installed within the customer's network. The TOE consists of a Microsoft Windows service called Core Installer and four Cloud Extender modules described in the table below which provides communications functionality with customer-provided services.

The diagram below is a high-level illustration of the TOE where the TOE is enclosed in the red dotted box.



The TOE consists of multiple processes running simultaneously. It uses the following cryptographic libraries:

- The Windows Cryptography API Next Generation (CNG) cryptographic library accessed via the .NET 4.7.2 framework.
- OpenSSL for the IBM MaaS360 Cloud Extender

CNG is used for communication and data-at-rest purposes while Open (Secure Sockets Layer) SSL is used for HTTPS connections. OpenSSL for the IBM MaaS360 Cloud Extender is also used to encrypt configuration templates generated by the IBM MaaS360 Cloud Extender Configuration Tool should TOE administrators wish to similarly configure another Cloud Extender. As this template is stored by default in an encrypted file system (EFS) volume, the TOE platform is thusly providing the overall data-at-rest capability.

The Core Installer communicates with the MaaS360 SaaS. It uses Client for URLs (cURL) and Windows crypto for protecting the communications channel between the MaaS360 SaaS application and the Cloud Extender. The Core Installer uses TLS 1.2 and initiates all communication with the MaaS360 SaaS application. Thus, the TOE acts as a TLS client.

The TOE is packaged with several third-party libraries which are listed in FPT_LIB_EXT.1. The IBM MaaS360 Cloud Extender Configuration Tool is supplied with the Cloud Extender installation package which can be used during the initial installation as well as on-demand when configuration changes are necessary.
The evaluated configuration includes four CE modules, which are packages of scripts and actions that integrate with components of the MaaS360 customer's infrastructure and provides full integration service with that component.

| **Cloud Extender Module** | **Description** |
|---|---|
| Exchange Integration for Active Sync Devices Module | The Exchange Integration module interacts with the Exchange Server to automatically discover ActiveSync-connected devices and uploads that device information to the MaaS360® Cloud.<br><br>The Exchange Integration module automatically quarantines devices, allows only MaaS360 enrolled devices, carries out actions (such as Approve, Block, or Remove device from the Mailbox) sent from MaaS360, and applies ActiveSync device policies.<br><br>This module supports MS Exchange 2007, 2010, 2013, 2016, Office 365,<br>and Microsoft Business Productivity Online Suite (BPOS)-D. |
| Corporate Directory | The User Authentication module interacts with Active Directory |

| | |
|---|---|
| Authentication Module | and 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.<br><br>The Cloud Extender supports integration with Lightweight Directory Access Protocol (LDAP) implementations, including Active Directory, Domino® LDAP, Oracle® LDAP, Novell® eDirectory LDAP, and OpenLDAP. |
| Corporate User Visibility Module | The User Visibility module synchronizes user and group information from LDAP or Active Directory directories to the MaaS360 SaaS application. |
| Certificate Authority Module | The Certificate Integration 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.<br><br>The Cloud Extender interacts with the CA, and then pushes the issued certificates down to enrolled devices by using the following method:<br>• It receives certificate requests from the MaaS360 Portal for all enrolled devices that require an identity certificate.<br>• It authenticates against the CA or Registration Authority (RA) as a part of the certificate request process.<br>• It requests ID certificates by passing the details of the device or user and corresponding attributes as a part of the certificate request.<br>• It encrypts the received certificate by using the public key of the requesting device and pushes the encrypted payload to the MaaS360 Portal, which is then delivered to the device.<br>• It supports auto-renewals of certificates and makes sure that devices receive the new certificates before the current certificate expires. |

## TOE Evaluated Configuration

The evaluation covers the following operating system and hardware configurations running the TOE.

- Operating system: Microsoft Windows Server 2019 Standard version 1809 (x64)

- Hardware: Dell PowerEdge R740 with an Intel Xeon Gold 5118 processor (SkyLake microarchitecture).

## Physical Scope of the TOE

The TOE is a Microsoft Windows application and delivered as an application installer executable.

## Un-evaluated Functionality

The following modules are not delivered with the TOE and therefore the services they provide are not part of the evaluated configuration:

- IBM Traveler module
- Exchange Integration for Real-time Mail Notifications module
- BlackBerry Enterprise Server (BES) module
- Mobile Enterprise Gateway (MEG) module
- MaaS360 VPN module
- Zebra Printer Management module

This section summaries the security functionality of the TOE including the following.

1. Cryptographic support
2. User data protection
3. Identification and authentication
4. Security management
5. Privacy
6. Protection of the TSF (TOE Security Functionality)
7. Trusted path/channels

## Cryptographic Support

The TOE provides cryptographic support using the Windows platform provided cryptographic services via the Cryptography API: Next Generation (CNG) for the following:

1. TLS connections: CNG is used by Secure Channel (SChannel), enabling the Cloud Extender to communicate with the Exchange Server, Domain Controller, and PKI Certificate Servers using HTTPS, limiting the protocol to TLS 1.2, and only using a subset of the TLS 1.2 ciphers.
2. Protecting data-at-rest using the Encrypted File System (EFS) for directory that contains all configuration and log information.
3. Encrypting registry entries using the Data Protection Application Programming Interface (DAPI).
4. Generating an Exchange Server certificate during the installation process.

The TOE comes with OpenSSL which provides the following services:

1. TLS connections to the MaaS360 Portal and SCEP certificate servers (HTTPS using cURL.)
2. Encryption of configuration profiles stored in an EFS directory
3. Device and user certificate generation for certificate signing requests to a SCEP server using the device and user templates. These requests are completed by the SCEP server and certificates returned to the TOE

## User Data Protection

The application provides user data protection services through restricting access by the application to only those platform-based resources (sensitive data repositories, and network communications) that are needed in order to provide the needed application functionality. Sensitive application data is encrypted using platform-provided encrypted file system (EFS) services, when stored in non-volatile memory, such as the hard disk drive(s).

## Identification and Authentication

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

## Security Management

The TOE provides the ability to set various configuration options for the TOE. These options are stored in the Windows Registry and are protected using the Data Protection Application Programming Interface (DPAPI).

During installation, the files installed on the TOE platform are allocated appropriate file-permissions, protecting the TOE and its data from unauthorized access.

## Privacy

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

## Protection of the TOE Security Functionality

The TOE uses only documented Windows APIs. The TOE is packaged with third party libraries, which are listed in the Security Target, to provide supporting functionality. The TOE does not write user-modifiable files to directories that contain executable files.

The TOE is compiled by IBM using stack buffer overrun protection. The TOE is packaged and delivered in the Microsoft Windows Application Software (.EXE) format that is signed with the Microsoft Sign Tool.exe using the Microsoft Authenticode process.

The TOE also provides Address Space Layout Randomization (ASLR) techniques and does not request memory mapping at explicit addresses.

### Trusted Path/Channels

The TOE protects all transmitted data between itself and another trusted IT product by using TLS v1.2 as trusted path/channels. Protocols used within these trusted channels may include additional protection and include HTTPS and LDAPS

## 4. Assumptions

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

- Protection Profile for Application Software, Version 1.3, 2019-03-01
- Functional Package for TLS, Version 1.1, 2019-03-01

That information has not been reproduced here and the respective documents should be consulted if there is interest in that material. Additionally, the Security Problem Description has been presented in the Security Target.

### Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the Protection Profile for Application Software, Version 1.3 and Functional Package for TLS, Version 1.1 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Section 3 lists functionality that is excluded from this evaluation. All other functionality provided by the product 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 clarification. This text covers some of the more important limitations and clarifications of this evaluation.

Note: 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 Protection Profile for Application Software and Functional Package for TLS, performed by the evaluation team.

## 5. Documentation

The following documentation was used as evidence for the evaluation of the TOE.

### Design Documentation

None

### Guidance Documentation

The following documentation was used as evidence for the evaluation.

| Reference | Document Name | Location |
|---|---|---|
| [CC-CFG] | IBM MaaS360 Cloud Extender NIAP Protection Profile Setup and Operations Guide, ver 1.0, 20 July 2022 | Identified at the NIAP PCL listing |
| [ADM_GUIDE] | IBM MaaS360 Cloud Extender Admin Guide, ver 1.0, 20 July 2022 | Identified at the NIAP PCL listing |

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

## 6. IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. The specific test configurations and test tools utilized may be found in the Assurance Activity Report (AAR) in Section 2.2.

### Developer Testing

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

### Evaluation Team Independent Testing

The test platform is a Dell PowerEdge R740 with Intel Xeon Gold 5118 processor (Skylake microarchitecture) as specified in the Security Target.

The test system was set up according to a setup strategy that followed the evaluated configuration requirements specified in the guidance, supplemented by configurations required to perform testing. The TOE is in the evaluated configuration at the start of each test.

The TOE is installed within a Microsoft Active Directory (AD) Environment within the atsec CCTL facility.
External services provided Microsoft Active Directory, LDAP, NDES CA, Microsoft Windows Server CA, Microsoft Simple Certificate Enrollment Protocol (SCEP) and Microsoft Exchange are also present in the Operational Environment.

The following software tools were used during testing:

- Wireshark network packet analyzer version 3.4.9 with libpcap was used during testing to monitor network traffic. (https://www.wireshark.org/)
- Microsoft Network Monitor version 3.4 (https://www.microsoft.com/en-us/download/4865)
- Nmap port scanning tool (version 6.47) was used to scan for open ports on the TOE (https://nmap.org/).
- OpenSSL s_server version 1.1.1g FIPS (https://www.openssl.org/)
- Microsoft Internet Information Services (IIS) within Windows Server 2019 as the base OS for all Windows services
- Microsoft Standalone SDK – Version 8.0 (https://developer.microsoft.com/en-us/windows/downloads/windows-8-sdk)
- Sysinternal Suite – Version (https://download.sysinternals.com/files/SysinternalsSuite.zip)
- procmon – Version 3.90
- VMMaP – Version 3.21
- Binscope – Version 2014 (https://www.microsoft.com/enus/download/details.aspx?id=44995)
- Microsoft Windows Server 2019 System Tools
- Signtool - https://docs.microsoft.com/en-us/windows/win32/seccrypto/signtool
- Icacls - https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/icacls
- Cygwin64 (https://www.cygwin.com/install.html)
- Microsoft WinDbg x64 (10.0.22621.1) - https://developer.microsoft.com/en-us/windows/downloads/windows-sdk/

# 7. Evaluated Configuration

The evaluated configuration consists of a software application, configured in accordance with the documentation specified in section 5.

# 8. 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.

All work units defined by CC Version 3.1 Revision 5 and CEM Version 3.1 Revision 5 and the [ASPPv1.3] and [TLSPKGv1.1] received a pass verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements as well as assurance activities. The evaluation was conducted based upon CEM Version 3.1 Revision 5. The evaluation determined the TOE to be CC Part 2 extended and Part 3 conformant, and to meet the assurance requirements defined by the [ASPPv1.3] and [TLSPKGv1.1].

## Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit and the assurance activity specified in the [ASPPv1.3] and [TLSPKGv1.1]. 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 IBM product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and the [ASPPv1.3] and [TLSPKGv1.1] and that the conclusion reached by the evaluation team was justified.

## Evaluation of the Development Documentation (ADV)

The evaluation team applied each ADV CEM work unit and assurance activity specified in [ASPPv1.3] and [TLSPKGv1.1]. The evaluation team assessed the documentation and found it adequate to aid in understanding how the TSF provides the security functions. The documentation consists of a functional specification contained in the Security Target and guidance documents.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, [ASPPv1.3] and [TLSPKGv1.1] and that the conclusion reached by the evaluation team was justified.

## Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit and assurance activity specified in the [ASPPv1.3] and [TLSPKGv1.1]. 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. Both the administrator and user 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 the [ASPPv1.3] and [TLSPKGv1.1] and that the conclusion reached by the evaluation team was justified.

## Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The ALC evaluation also ensured the TOE is identified such that the consumer can identify the evaluated TOE.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and the [ASPPv1.3] and [TLSPKGv1.1] and that the conclusion reached by the evaluation team was justified.

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

The evaluation team applied each ATE CEM work unit and assurance activity specified in the [ASPPv1.3] and [TLSPKGv1.1]. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. The evaluation team performed an independent set of tests as mandated by the Assurance activities specified in the protection profiles.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and the [ASPPv1.3] and [TLSPKGv1.1] and that the conclusion reached by the evaluation team was justified.

## Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit and assurance activity specified in the [ASPPv1.3] and [TLSPKGv1.1]. The vendor provided security updates to the TOE during the evaluation, [ASPPv1.3] and [TLSPKGv1.1] updates, in line with the guidance provided in Scheme Policy Letter 15, fixed all known issues. The evaluation team ensured that the currently available version of the TOE does not contain known exploitable flaws or weaknesses in the TOE based upon the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

The evaluators searched for publicly known vulnerabilities applicable to the TOE using the following sources:

- Common Vulnerabilities and Exposures (CVE)
  https://cve.mitre.org/cve/cve.html
- Cypersecurity and Infrastructure Security Agency (CISA)
  https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- OpenSSL website
  https://www.openssl.org/news/vulnerabilities.html
- The developer's support website for security publications
  https://www.ibm.com/mysupport

Note that the latest search was performed on September 12, 2022 using the following search terms:

- IBM MaaS360 Cloud Extender
- Microsoft Windows Server 2019 Standard version 1809 (x64)
- TLS 1.2
- XMPP (Extensible Messaging and Presence Protocol)

- Exchange Integration for Active Sync Devices Module
- Corporate Directory Authentication Module
- Corporate User Visibility Module
- Certificate Authority Module
- Windows Cryptography API: Next Generation
- .NET 4.7.2

The evaluator found no vulnerabilities applicable to the TOE that could be exploited by a Basic Attack Potential or that required any additional testing apart from the evaluator's normal independent testing.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and the [ASPPv1.3] and [TLSPKGv1.1] and that the conclusion reached by the evaluation team was justified.

### 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 performance of the testing defined by the [ASPPv1.3] and [TLSPKGv1.1] and the penetration test also demonstrated the accuracy of the claims in the ST.

The validator'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 the [ASPPv1.3] and [TLSPKGv1.1] and correctly verified that the product meets the claims in the ST.

## 9. Validator Comments/Recommendations

All of the validators concerns are adequately captured in Section 4, Assumptions and Clarification of Scope.

## 10. Annexes

Not applicable.

## 11. Security Target

IBM MaaS360 2.106.500.016 Cloud Extender Security Target, Version 1.4, dated 2022-07-20

# 12. Glossary

The following definitions are used throughout this document.

| | |
|---|---|
| **AA** | Assurance Activity |
| **CC** | Common Criteria |
| **CCEVS** | Common Criteria Evaluation and Validation Scheme |
| **CCTL** | Common Criteria Testing Laboratory—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. |
| **CEM** | Common Criteria Evaluation Methodology |
| **Conformance** | The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model. |
| **ETR** | Evaluation Technical Report |
| **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. |
| **NIAP** | National Information Assurance Partnership |
| **NSA** | National Security Agency |
| **NVLAP** | National Voluntary Laboratory Assessment Program |
| **PP** | Protection Profile |
| **SFR** | Security Functional Requirement |
| **ST** | Security Target |
| **TOE** | Target of Evaluation—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. |
| **TLS** | Transport Layer Security |
| **TSF** | TOE Security Functionality |
| **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. |
| **VR** | Validation Report |

# 13. Bibliography

The evaluation team used the following documents to produce this Validation Report:


- Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.
- Protection Profile for Application Software, Version 1.3, 2019-03-01
- Functional Package for Transport Layer Security (TLS), Version 1.1, 2019-03-01.
- MaaS360 Cloud Extender Admin Guide, v1.0, 2022-07-20.
- MaaS360 Cloud Extender Common Criteria Guide, v1.0, 2022-07-20.
- IBM MaaS360 2.106.500.016 Cloud Extender Security Target, Version 1.4, 2022-07-20
- Assurance Activity Report, Version 1.0, 2022-09-12